TP2B THE PLACE TO BE

ATEA

INFOTURBE RISKIJUHTIMINE: TÖÖTAJATELE KOHALDATAVAD PÕHIMÕTTED

Versioon 1.0 – avaldatud august 2019

KIRI TEGEVJUHILT

Atea missioon on „ehitada IT abil tulevikku“ (Build the Future with IT).

Usume, et infotehnoloogia üheskoos teadmiste ja loovusega suudab tõsta tootlikkust ja elatustaset kogu ühiskonnas. Toetame ettevõtjaid ja avaliku sektori organisatsioone digilahenduste leidmisel, mis võimaldab neil tõhusamalt ja väiksema ressursikuluga rohkem saavutada.

Samas mõistame riske, mis tulenevad tehnoloogiast, mis suudab salvestada ja töödelda aina rohkem teavet. Sedamööda, kuidas organisatsioonid käsitlevad aina rohkem andmeid ja automatiseerivad protsesse oma IT-süsteemides ja võrkudes, seisavad nad silmitsi suurema andmevarguse, identiteedipettuse ning küberrünnakute põhjustatud tegevuskatkestuste riskiga. Andmetega seotud rikkumise tulemusel võidakse saada juurdepääs inimese andmetele ilma tema nõusolekuta ja neid andmeid võidakse sellele isikule kahju tegemiseks ja tema eraelu puutumatuse õiguse rikkumiseks väärkasutada.

Atea on Põhjamaades ja Balti riikides juhtiv infotehnoloogia pakkuja, kellel lasub eriline vastutus tagada tegevuse vastavus infoturbe rangetele standarditele. Atea kavandab, rakendab ja käitab IT-taristu lahendusi meie piirkonna suurimatele ja kõige olulisematele organisatsioonidele. Suur osa meie käibest tuleneb riigiasutustest ja kohalikest omavalitsustest, muu hulgas sellistelt väga tundlikelt klientidelt nagu sõjavägi ja politsei. Samuti pakume piirkonna suurimatele ettevõtetele eluliselt tähtsaid IT-lahendusi.

See dokument sisaldab suuniseid, kuidas Ateas infoturbega seotud riske juhtida. Selles antakse ülevaade peamistest turberiskidest, andmekaitse põhimõtetest ning õiglasest menetlusest, mis mõjutavad kõiki meie ettevõttes. Töötajad, kellel on seoses IT-tegevuse ja süsteemihaldusega erikohustused, peavad vastavalt oma ametikohustustele tutvuma infoturbe ja andmekaitse põhimõtetega eraldi ja põhjalikumalt.

Dokument on jagatud neljaks osaks. Iga osa lõpus tehakse sellest kokkuvõte. Need neli osa on üksikasjalikud, kuna tegemist on keerulise ja ärikriitilise teemaga. On eriti tähtis, et töötajad jätaksid meelde iga osa lõpus olevas kokkuvõttes esitatud punktid ning on vajaduse korral võimelised leidma muud dokumendis sisalduvat teavet.

Selle dokumendi sisu peavad teadma kõik Atea töötajad. Tagamaks, et kõik Atea töötajad saavad selle dokumendi sisust aru, on toimimisjuhendit käsitlevasse eksamisse (mis on kõigile Atea töötajatele kohustuslik) lisatud kümme küsimust infoturbe kohta. Töötajatel on võimalik läbida internetipõhine koolitus, et tutvuda Atea infoturbealaste põhimõtetega ja valmistuda toimimisjuhendit käsitlevaks eksamiks.

Steinar Sønsteby
tegevjuht

Atea on suur organisatsioon, kes tegutseb seitsmes riigis, kus on ligikaudu 90 esindust. Kontsern on määranud endale ja iga tegevuskoha riigi jaoks infoturbe juhi, kes toetab infoturbe põhimõtete rakendamist kogu Atea organisatsioonis.

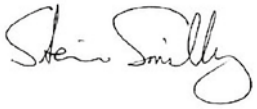
Kui teil on Atea infoturbe kohta küsimusi või muresid, palume need esitada järgmiselt.

- Kui arvate, et teie arvuti võib olla nakatunud pahavaraga, või kui teil on üldisi küsimusi IT-turvalisuse kohta, võtke ühendust Atea teenindustoega.
- Kui soovite teatada kahtlasest e-kirjast, pettuse katsest või muust sündmusest, mis võib kujutada Ateale infoturberiski, võtke ühendust Atea teenindustoega.
- Kui soovite teatada kahtlusest, et infosüsteemides või dokumentides on toime pandud isiku- või äriandmetega seotud rikkumine (omavoliline avalikustamine), võtke ühendust selle riigi, kus töötate, infoturbe juhiga. Alternatiivselt võite saata e-kirja otse aadressile infosec@atea.com.

Kui soovite rääkida otse Atea kontserni või oma riigi või ühise teenindusüksuse infoturbe juhiga (CISO), leiate vastavate isikute nimed Atea nõuetele vastavuse veebisaidilt atea.com/trust. Kõik aadressile infosec@atea.com saadetud e-kirjad edastatakse otse Atea kontserni infoturbe juhile.

Meil on hea meel saada teilt küsimusi ja tagasisidet ning lubame, et probleemidest teatamisel ei rakendata teie suhtes survemeetmeid. Kuid kui teil on mure, millest eelistate teatada anonüümselt, võite selleks kasutada rikkumistest teavitamise vihjeliini (Whistleblower Hotline). Lingi rikkumistest teavitamise vihjeliinile leiab Atea nõuetele vastavuse veebisaidilt atea.com/trust. Rikkumistest teavitamise vihjeliinile jäetud probleem edastatakse sõltumatule õigusbüroole, kes teeb sellest kokkuvõtte ja saadab selle asjakohasele Atea organisatsiooni juhtimistasemele.

Infoturbe rangete standardite säilitamine on Atea äritegevuses oluline, samuti on see tähtis selleks, et saaksime töötada koos klientide ja partneritega meie piirkonna kõige olulisemate IT-alaste proovikivide lahendamiseks. Täname teid Atea infoturbe põhimõtete järgimise ja selle eest, et olete aidanud muuta Atea „kohaks, kus olla“.



Olulised punktid:

Atea jaoks on väga tähtis, et kõik töötajad säilitaksid infoturbe ranged standardid.

Kontsern on määranud endale ja iga tegevuskoha riigi jaoks infoturbe juhi, kes toetab infoturbe põhimõtete rakendamist kogu Atea organisatsioonis. Infoturbe juhtide nimed leiab Atea nõuetele vastavuse veebisaidilt: atea.com/trust.

Kui teil on Atea infoturbe kohta küsimusi või sellega seotud muresid, palume need edastada meile järgmiselt.

- Kui arvate, et teie arvuti võib olla nakatunud pahavaraga, või kui teil on üldisi küsimusi IT-turvalisuse kohta, võtke ühendust Atea teenindustoega.
- Kui soovite teatada kahtlasest e-kirjast, pettuse katsest või muust sündmusest, mis võib kujutada Ateale infoturberiski, võtke ühendust Atea teenindustoega.
- Kui soovite teatada kahtlusest, et infosüsteemides või dokumentides on toime pandud isiku- või äriandmetega seotud rikkumine (omavoliline avalikustamine), võtke ühendust selle riigi, kus töötate, infoturbe juhiga.
- Alternatiivselt võite saata e-kirja aadressile infosec@atea.com, kuhu laekuvad e-kirjad edastatakse kõik otse Atea kontserni infoturbe juhile.

Toimimisjuhend

1. INFOTURVE – ÜLEVAADE JA RISKIJUHTIMINE

Teave on iga organisatsiooni toimimise jaoks väga oluline. Infoturbe juhtimise süsteem (information security management system (ISMS)) kujutab endast põhimõtete, menetluste, vahendite ja tegevuste kogumit, mida organisatsioon kasutab oma teabevara kaitsmiseks omavolilise juurdepääsu ja väärkasutamise eest.

ISMSi juurutamiseks peab organisatsioon tuvastama tema valduses oleva teabevara. See hõlmab kõiki andmeid, mida organisatsioon käsitleb nende vormist sõltumata: digitaalsed, paberkandjad või suulised andmed. Ateas võib selline teave olla mõeldud sisekasutuseks; samas võib olla tegu ka ettevõtteväliste andmetega, mida Atea haldab ja töötleb kliendile osutatava teenuse raames.

ISMSi eesmärk on kaitsta ja hoida teabevara konfidentsiaalsust, terviklikkust ja kättesaadavust.

- **Konfidentsiaalsus** tähendab, et teave on kättesaadav ainult volitatud isikutele.
- **Terviklikkus** tähendab, et teavet hoitakse selliselt, et see on täielik ja õige.
- **Kättesaadavus** tähendab, et volitatud kasutajad saavad vajaduse korral andmetele juurde pääseda ja neid kasutada.

Kõnealuste eesmärkide saavutamiseks peaks organisatsioon viima läbi riskihindamise, et teha kindlaks, kuidas võimalikud infoturbe riskid võivad selle teabevara ohustada. Seejärel saab organisatsioon koostada ISMSi, mis aitab selliseid riske tõhusalt juhtida ja ohjata ilma ebavajalike kulusid või tootmiskadusid kaasa toomata.

Riskihindamine Ateas

Järgmised infoturbega seotud riskid on tuvastatud kui Atea äritegevusele kõige olulisemad.

1. **Füüsiline kadu:**
   teabevara hoitakse füüsilistel kandjatel, mis võivad kaduma minna ja mida võidakse varastada või kahjustada. Juurdepääsu kontroll, krüptimine ja andmevarundus on seetõttu hädavajalikud, et piirata füüsilise varaga, näiteks arvutite, mobiiltelefonide, serverite ja salvestamisega seotud riskide võimalust. Eriti haavatavad on andmekeskused, mida tuleb kaitsta ka selliste keskkonnaohtude nagu temperatuurimuutused ja põlengud eest.

2. **Identiteedipettus:**
   Ateat ohustavad pidevalt pettusekatsed ründajate poolt, kes kasutavad töötajate usalduse võitmiseks variidentiteeti või eksitamist. Tavaliselt on pettusekatse eesmärk Atealt varastamine või Atea süsteemidele ja võrkudele volitamata juurdepääsu saamine.

   Üks Atea-vastase identiteedipettuse vorme on valede või varastatud kliendikonto andmete kasutamine IT-seadmete tellimiseks, eelkõige Atea Eshopist. Lisaks Eshopis kasutatavatele juurdepääsu kontrollidele on Ateas paigas toimingud uute kliendikontode kontrollimiseks ja olemasolevatel kontodel ebatavalise klienditegevuse tuvastamiseks, et vähendada pettusega seotud klienditehingute riski.

   Üks teine levinud identiteedipettus (andmepüük) on olukord, kus ründaja võtab Atea töötajaga otse, tavaliselt e-posti kaudu, ühendust. E-kiri on pealtnäha usaldusväärsest allikast; sageli kasutatakse valesid isikuandmeid, näiteks mõne teise Atea töötaja, äripartneri või sellise tarnija nagu tehnoloogiaettevõtte või panga andmeid. E-kirjaga üritatakse Atea töötajat veenda vastama, näiteks kandma üle raha, avaldama sisselogimise / salasõna andmed või muud tundlikku teavet või klõpsama lingil või manusel, mis laadib kasutaja arvutisse või mobiiltelefoni kahjuliku tarkvara (nn pahavara).

   E-kiri, manus või link on pealtnäha ohutu – näiteks võib see olla maskeeritud kui kolleegi saadetud e-kiri, pakkumine/arve tarnijalt või teavitus selliselt pilvekontolt nagu OneDrive. Seetõttu peavad Atea töötajad olema äärmiselt valvsad e-posti ja muu teabevahetusega seotud võimalike pettuste suhtes – ka siis, kui sõnum tundub olevat usaldusväärsest allikast.

   Atea töötajad ei tohiks kunagi avada oma seadmes linke või manuseid, kui nad kahtlevad e-kirja või teavituse õiguspärasuses. Kui Atea töötajal peaks olema kahtlusi e-kirja õiguspärasuse suhtes või kui ta on kogemata

kahtlase lingi või manuse avamisega vastanud võimalikule pettusekatsele, peaks ta võtma kohe ühendust Atea teenindustoega ja probleemist teada andma.

E-post on tööga seotud andmepüügi kõige levinum meetod, kuid Atea töötajad peaksid olema valvsad ka muude pettusega seotud teabevahetuse vormide suhtes, sealhulgas telefonikõnede ja sotsiaalmeedia kaudu saadetud kutsete suhtes.

3. Ärisaladuste vargus:
kui volitamata isik saab juurdepääsu Atea infosüsteemidele, võib ta üritada varastada Atea äritegevusest tundlikku ärisaladuse alla kuuluvat informatsiooni. Selleks võib olla salajane äriteave, näiteks klientide või varustajate andmed ning kaubandustingimused. Selleks võivad olla ka intellektuaalomandi õigused, näiteks ärikontseptsioonid, toodete või teenuste disainilahendused ning ettevõtte siseselt välja töötatud tarkvara, meetodid ja vahendid.

Töötajad, kellel on juurdepääs põhisüsteemidele, võivad üritada Atealt varastada ärisaladusi, eriti juhul, kui neil on kavas ettevõttest lahkuda. Riski vähendamiseks tohib töötajatele anda teabele juurdepääsu üksnes teadmisvajaduse alusel. Süsteemile juurdepääsu tuleb pidevalt jälgida, et tagada teadmisvajaduse põhimõtte järgimine, ning kasutaja juurdepääsuõigus tuleb lõpetada kohe, kui tal pole seda õigust enam kasutada vaja.

Lisaks juurdepääsu kontrollile kasutab Atea turbeinfo ja sündmuste halduse süsteemi (Security Information and Event Management (SIEM)) vahendeid sisselogimisteabe ja süsteemis aset leidnud tegevuste analüüsimiseks.

4. Majandustegevuse katkemine:
Atea majandustegevus sõltub tema IT-süsteemidest. Juurdepääsu kontrollide rikkumisel või süsteemide väärkasutamisel võib töötajate või äripartnerite valduses olev privaatne teave lekkida. Atea majandustegevuses vajalikku teavet võidakse lubamatult muuta või kustutada. Viimaseks – Atea haldamise kontrollisüsteemi rikkudes võivad volitamata isikud sõlmida või kiita heaks äritehinguid. Igasugune selline tegevus häirib Atea majandustegevust.

Ateat ohustab ka tegevuse katkemine keeruka häkkimisrünnaku tagajärjel, kui peamised IT-süsteemid või -võrgud võivad minna rivist välja. Süsteeme võidakse nakatada pahavaraga, mis ei lase kasutajatel pääseda ligi kriitilise tähtsusega funktsioonidele, või mis takistab andmefailide lugemist, kui ei maksta lunaraha (nn lunavara). Võrgud või serverid võidakse ujutada üle liikluse või taotlustega, nii et õiguspäraseid tehinguid ei ole enam võimalik käsitleda (nn teenust tõkestav rünnak). Selliste rünnakute sihtmärk võib olla Atea ise või kliendid, keda Atea oma andmekeskuse kaudu haldab.

5. Lepinguline kahju:
Atea on sõlminud paljude klientide, tarnijate ja äripartneritega konfidentsiaalsuslepingud. Atea on ühtlasi sõlminud Atea IT-teenuseid ja -tuge kasutavate klientidega teenindustaseme ja andmetöötluslepingud.

IT-turbega seotud vahejuhtumi tagajärjel võib Atea rikkuda klientide ja teiste äripartneritega sõlmitud konfidentsiaalsus-, teenindustaseme ja andmetöötluslepinguid. Atea võidakse kaevata kohtusse lepingu rikkumisest tingitud kahjude hüvitamiseks. Lisaks otsestele kahjudele võib IT-turbega seotud vahejuhtum jäädavalt kahjustada Atea suhteid klientide ja partneritega.

Isegi kui Ateal ei ole konkreetset lepingut sõlmitud, võib Atea seista silmitsi õigusnõuetega ettevõtjatelt või eraisikutelt, kelle andmeid on varastatud või väärkasutatud, kui Atea ei tõenda, et tegutseb andmete käsitlemisel nõuetekohase hoolsusega.

6. Õigusnormides ette nähtud sanktsioonid:
Oslo börsil noteeritud äriühinguna peab Atea turul üldiselt mitteteadaolevate ja Atea aktsiahinda mõjutada võivate andmete (nn hinnatundlik teave) käsitlemisel järgima rangeid juriidilisi nõudeid. Selline teave võib puudutada uusi mahukaid lepinguid või finantstulemusi, millest üldsust veel teavitatud ei ole.

Atea peab hinnatundlikku teavet käsitlema konfidentsiaalselt, et tagada, et selline teave ei leviks kaugemale registreeritud ja teadmisvajaduse alusel siseteavet valdavate isikute piiratud ringist. Hinnatundlikku teavet valdavad töötajad peavad olema ettevõtte poolt registreeritud ja nende suhtes kehtivad spetsiaalsed vaikimisnõuded ning Atea aktsiatega kauplemise piirangud. Nende õigusnõuete rikkumisel võidakse esitada süüdistus ja rakendada sanktsioone Norra väärtpaberitega kauplemise seaduse alusel.

Ühtlasi võidakse vastavalt Euroopa Liidu isikuandmete kaitse üldmäärusele (isikuandmete kaitse üldmäärus) rakendada Atea suhtes isikuandmetega seotud rikkumiste eest õigusnormides ette nähtud sanktsioone. Kuna isikuandmete kaitse üldmääruse nõuded on üsna ulatuslikud, siis lahatakse seda teemat pikemalt selle dokumendi järgmises, andmete privaatsust käsitlevas osas.

Olulised punktid:

kõik töötajad peavad teabe ja IT-süsteemide käsitlemisel olema äärmiselt hoolikad, et hoida ära infoturbega seotud rikkumisi.

IT-seadmed võivad kaduma minna ja neid võidakse varastada või kahjustada. Juurdepääsu kontroll, krüptimine ja andmevarundus on seetõttu hädavajalikud, et piirata infoturbega seotud riskide võimalust.

Ateat ohustavad pidevalt pettusekatsed ründajate poolt, kes kasutavad töötajate usalduse võitmiseks variidentiteeti või eksitamist. Peate teadma, et iga saadud e-kiri või muu teavitus võib olla pettusekatse, isegi kui see on pealtnäha õiguspärasest allikast (kaasa arvatud kirjad Atea juhtidelt, klientidelt, tehnoloogia tarnijatelt või sotsiaalmeedia kontodelt).

Olge valvas igasuguse ebatavalise teabevahetuse või tegevuse suhtes, mille tunnistajaks võite olla. Kui kahtlustate, et teist on e-kirja või muu sõnumi kaudu saanud pettuse sihtmärk, võtke oma murega ühendust Atea teenindustoega. Ärge vastake kahtlasele sõnumile – näiteks e-kirja manuse või välislingi avamise või tellimuse/makse töötlemisega.

Töötajatele tohib anda teabele juurdepääsu üksnes teadmisvajaduse alusel, et ennetada teabe varastamise või väärkasutamise riski. Süsteemile juurdepääsu tuleb pidevalt jälgida, et tagada kasutaja juurdepääsuõiguse lõpetamine kohe, kui tal pole seda õigust enam kasutada vaja.

Infoturbega seotud vahejuhtumid võivad tõsiselt Ateat kahjustada majandustegevuse katkemise, klientide ja äripartnerite ees olevate lepinguliste kohustuste rikkumise, õigusnormides ette nähtud sanktsioonide ning Atea maine ja ärisuhete kahjustamise tõttu.

2. ANDMETE PRIVAATSUS – ÜLEVAADE JA RISKIJUHTIMINE:

Andmete privaatsus tähendab, et isikul on oma andmete üle kontroll – konkreetsemalt on tal võimalik otsustada, kus ja millal tema andmeid kogutakse, jagatakse ja kasutatakse. Isikuandmeid määratletakse kui mis tahes teavet ükskõik millises vormis, mis viitab konkreetsele ja tuvastatavale isikule.

Andmete privaatsus sõltub infoturbest, st sellest, kuidas andmeid kaitstakse omavolilise juurdepääsu ja väärkasutamise eest. Andmete privaatsus ulatub siiski infoturbest kaugemale – see tähendab ka inimese isikuandmete omamise õiguse kaitset. Konkreetsemalt – kuidas tagab organisatsioon igale töötajale võimaluse kontrollida tema isikuandmete töötlemist, kui organisatsioon selle töötaja kohta andmeid kogub ja töötleb?

Ateas usume, et andmete privaatsus on põhiõigus ja oleme pühendunud isikuandmete käsitlemisele viisil, mis seda põhimõtet täielikult järgib. Atea suhtes kehtivad isikuandmete töötlemisel ranged juriidilised nõuded vastavalt Euroopa Liidu isikuandmete kaitse üldmäärusele (isikuandmete kaitse üldmäärus).

Isikuandmete kaitse üldmääruse nõuded, mis Ateale kohalduvad, on kokkuvõtlikult järgmised.

Nõuded isikuandmete kogumisele
Atea võib isikuandmeid töödelda (st koguda, salvestada ja kasutada), kui tal on selleks õigustatud ärihuvi ja kui asjaomane isik on andnud selleks nõusoleku või kui teda on isikuandmete töötlemisest teavitatud. Sellist teavitamist või nõusoleku andmist on põhjalikumalt kirjeldatud selle dokumendi järgmises osas.

Inimese õigus omada oma isikuandmete üle kontrolli
Atea peab täitma isiku taotluse oma isikuandmete kasutust kontrollida vastavalt talle isikuandmete kaitse üldmääruses antud andmete privaatsuse õigusele. Kooskõlas isikuandmete kaitse üldmäärusega on inimesel õigus juurdepääsule Atea valduses selle isiku kohta olevatele isikuandmetele. Inimesel on samuti õigus lasta oma isikuandmeid parandada, kustutada või piirata nende töötlemist ja kasutamist.

Andmetöötluse dokumenteerimine
Atea peab dokumenteerima, millises ulatuses ta isikuandmeid töötleb. See peaks sisaldama töödeldavate isikuandmete liikide ja isikute kategooriate kirjeldust. Ühtlasi peaks see hõlmama kirjeldust sellest, milliseid tehnilisi ja korraldusliikke meetmeid on võetud andmetega seotud rikkumiste ennetamiseks ja nende mõju vähendamiseks Atea andmetöötlusalases tegevuses (nn lõimitud andmekaitse).

Andmetöötluslepingud klientide/tarnijatega
Kui Atea pakub klientidele andmetöötlusteenuseid (nt kui Atea haldab kliendi jaoks andmeteristut ja rakendusi kas kliendi juures kohapeal või oma andmekeskuse kaudu), siis peab Ateal olema ka kehtiv kliendiga sõlmitud andmetöötlusleping, mis vastab isikuandmete kaitse üldmääruse nõuetele.

Samamoodi – kui Atea töötleb isikuandmeid alltöövõtja või tarnija kaudu (nt kui ta kasutab tarnija andmekeskuses käitatavaid tarkvararakendusi, näiteks pilveteenuseid), peab Ateal olema kehtiv ja isikuandmete kaitse üldmääruse nõuetele vastav andmetöötlusleping ettevõttega, kes haldab Atea nimel isikuandmete kasutamist ja töötlemist. Väljaspool ELi/EMPi töödeldavate andmete puhul peab töötlemine toimuma riigis või raamistikus, mille kohta on riigiasutused otsustanud, et seal kehtivad piisavad andmekaitsemeetmed.

Nõuded andmetega seotud rikkumise korral
Isikule kahju tekitada võiva andmetega seotud rikkumise korral peab Atea 72 tunni jooksul rikkumisest teada saamisest teavitama järelevalveasutust riigis, kus andmetega seotud rikkumine aset leidis. Teade peab kirjeldama rikkumise laadi, sisaldama seotud andmesubjektide ja registrite kokkuvõtet, rikkumise tõenäolisi tagajärgi ning kasutusele võetavaid meetmeid.

Teavitada tuleb ka isikut, kelle isikuandmetega seoses rikkumine toime pandi, kui on suur sellele isikule kahju tekkimise oht. Kui isikut ei ole võimalik individuaalselt teavitada, piisab ka avalikust teadaandmisest.

Kooskõlas isikuandmete kaitse üldmäärusega on riigi järelevalveasutusel õigus isikuandmete kaitse üldmääruse rikkumisel määrata ettevõtjale suur trahv. Trahvi suurus sõltub rikkumise laadist, andmete privaatsusega õiguste rikkumise ulatusest ja meetmetest, mida ettevõte on võtnud rikkumiste ennetamiseks ja kõrvaldamiseks. Maksimaalne trahv isikuandmete kaitse üldmääruse rikkumise eest on 4% globaalsest aastatulust või 20 miljonit eurot, olenevalt sellest, kumb on suurem.

Isikuandmete kaitse üldmääruse nõuete alusel on äärmiselt oluline, et Atea dokumenteeriks kõik rutiinid, mis hõlmavad isikuandmeid, ning tuvastaks kõik isikuandmeid sisaldavad ettevõttesisesed rakendused ja lepingud. See teave peab olema kättesaadav iga riigi infoturbe juhile, et saada kinnitust selle kohta, et andmete privaatsuse kaitseks on rakendatud asjakohaseid meetmeid. Iga riigi ja kontserni infoturbe juhi andmed leiab Atea nõuetele vastavuse veebisaidilt.

Olulised punktid:

andmete privaatsus tähendab, et isikul on oma andmete üle kontroll – konkreetsemalt on tal võimalik otsustada, kus ja millal tema andmeid kogutakse, jagatakse ja kasutatakse. Isikuandmeid määratletakse kui mis tahes teavet ükskõik millises vormis, mis viitab konkreetsele ja tuvastatavale isikule.

Atea suhtes kehtivad isikuandmete töötlemisel ranged juriidilised nõuded vastavalt Euroopa Liidu isikuandmete kaitse üldmäärusele (isikuandmete kaitse üldmäärus).

Vastavalt isikuandmete kaitse üldmäärusele:

Atea võib isikuandmeid töödelda (st koguda, salvestada ja kasutada), kui tal on selleks õigustatud ärihuvi ja kui asjaomane isik on andnud selleks nõusoleku või kui teda on isikuandmete töötlemisest teavitatud.

Atea peab täitma isiku taotluse oma isikuandmete kasutust kontrollida vastavalt talle isikuandmete kaitse üldmääruses antud andmete privaatsuse õigusele.

Atea peab dokumenteerima, millises ulatuses ta isikuandmeid töötleb, sealhulgas kirjeldama meetmeid, mida võetakse andmetega seotud rikkumiste ennetamiseks ja nende mõju vähendamiseks. See tähendab, et Atea peaab dokumenteerima kõik rutiinid, mis hõlmavad isikuandmeid, ning tuvastama kõik isikuandmeid sisaldavad ettevõttesisesed rakendused ja lepingud.

Ateal peavad olema sõlmitud kehtivad andmetöötluslepingud kõigi klientidega, kellele ta pakub andmetöötlusteenuseid (nt klientide jaoks andmetaristu ja rakenduste haldamine kas koha peal kliendi juures või oma andmekeskuse kaudu).

Ühtlasi peavad Ateal olema kehtivad andmetöötluslepingud kõigi alltöövõtjate või tarnijatega, kes Atea nimel isikuandmeid töötlevad (nt tarkvararakenduste ja andmesalvestuse pakkumine tarnija andmekeskus, nt pilveteenuste pakkumine).

Isikule kahju tekitada võiva andmetega seotud rikkumise korral peab Atea 72 tunni jooksul rikkumisest teada saamisest teavitama järelevalveasutust riigis, kus andmetega seotud rikkumine aset leidis.

3. ATEA ANDMEKAITSE PÕHIMÕTTED

Atea töötajad peavad andmete kogumisel, käsitlemisel ja levitamisel alati järgima ettevõtte andmekaitse põhimõtteid. Kõik Atea juhid on kohustatud tagama, et nende vastutusvaldkonda jäävad äriprotsessid on vastavuses Atea andmekaitse põhimõtetega, ja et nende alluvad järgivad oma töös neid põhimõtteid.

Kõigile Atea juhtidele on määratud andmekaitse haldur, kes vastutab oma riigis (või ühise teenindusüksuses) konkreetse ärifunktsiooni eest. Andmekaitse halduri roll on kontrollida, kas kõik funktsiooni äriprotsessid vastavad Atea andmekaitse põhimõtetele. Sellisteks funktsioonideks on: müük/turundus, personal, rahandus, konsultatsiooniteenused, AMS, logistika ja IT.

Iga funktsiooni andmekaitse haldur allub riigi (või ühise teenindusüksuse) infoturbe juhile. Iga riigi infoturbe juhil lasub üldvastutus selle riigi andmekaitse põhimõtete täitmise eest. Riigi infoturbe juht allub kontserni infoturbe juhile.

Oma riigi infoturbe korralduse kõigi olulisemate liikmete kontaktandmed leiate Atea nõuetele vastavuse veebisaidilt atea.com/trust. Kokkuvõtte infoturbe korraldusest leiab ka selle dokumendi lisast.

Atea andmekaitse põhimõtted hõlmavad järgmist:

- süsteemi registreerimine
- andmete klassifitseerimine
- isikuandmete haldamine
- kliendilepingud

Ülevaade andmekaitse põhimõtetest.

Süsteemi registreerimine

Enne kui Atea töötaja saab asuda teavet koguma, käsitlema või jagama, peab ta kinnitama, et kõik infosüsteemid, milles andmeid salvestatakse või töödeldakse, on riigi infoturbe juhi juures registreeritud ja tema poolt heaks kiidetud. See hõlmab pilveteenuseid, mida ostetakse liitumiste kaudu ja hallatakse väljaspool Ateat.

Infoturbe juht analüüsib enne infosüsteemi Ateas kasutamiseks registreerimist süsteemi IT-turvalisuse ja andmete privaatsuse standardeid. Analüüsimisel lähtub ta Atea kontserni IT-turvalisuse ja andmekaitse standardite kontrollinimekirjast, mille ta täidab koos Atea kontserni infoturbe juhiga.

Infoturbe juht arvestab süsteemi Atea infoturbe nõuetele vastavust analüüsides ka süsteemi salvestatavate andmete liiki ja tundlikkust. Ühe osana analüüsist kinnitab infoturbe juht põhimõtted isikuandmete süsteemist kustutamiseks, kui Atea neid andmeid enam ei vaja (nn andmete minimeerimise põhimõtted).

Kui infosüsteemi hallatakse ettevõtteväliselt ja see sisaldab isikuandmeid, näiteks pilvepõhine personalihalduse süsteem, siis peab Atea isikuandmete kaitse üldmäärusele vastamiseks sõlmima teenuseosutajaga andmetöötluslepingu (data processing agreement (DPA)). Pilveteenuste osutajaga sõlmitava standardse DPA leiate oma riigi intraneti globaalse infoturbe veebilehelt. Iga riigi infoturbe juht vastab DPAd puudutavatele küsimustele ja saab pakkuda abi teenuseosutajalt allkirjastatud DPA hankimise protsessis.

Atea töötajad ei tohi ettevõtte andmeid salvestada ega töödelda nn variinfotehnoloogiasüsteemides, mis ei ole nende riigi infoturbe juhi juures registreeritud. Atea töötajad ei tohi andmete käsitlemise süsteeme ega protsesse oluliselt muuta ilma sellest infoturbe juhti teavitamata, et IT-turvalisust oleks võimalik uuesti hinnata.

Kui süsteem on Ateas kasutamiseks lubatud, määratakse süsteemile süsteemiomanik. Süsteemiomanik vastutab selle eest, et oleks tagatud süsteemi kasutamine vastavalt Atea andmekaitse põhimõtetele. Konkreetselt peab süsteemiomanik tagama, et infosüsteemile juurdepääsu õigusi antakse ainult teadmisvajaduse baasil ja need lõpetatakse kohe, kui neid enam vaja ei ole. Ühtlasi peab süsteemiomanik tagama, et süsteemis salvestatud isikuandmed kustutatakse, kui Atea neid enam ei vaja, kooskõlas andmete minimeerimise põhimõtetega, milles lepiti kokku süsteemi kasutamise kooskõlastamisel.

Andmete klassifitseerimine
Kui süsteem lubatakse Ateas kasutusse, dokumenteeritakse süsteemis salvestatavate andmete liik ja tundlikkust, et tagada asjakohaste andmekaitse põhimõtete hoidmine.

Sageli võivad Atea töötajad siiski käsitleda ja jagada teavet väljaspool volitatud IT-süsteemi. See hõlmab teavet, mille käsitlemiseks kasutatakse väljaprinditavaid dokumente e-posti teabevahetuse e-posti teel või failide jagamise kaudu (st Microsoft Wordi/Exceli/Powerpointi failid).

Selleks, et tagada, et väljaspool volitatud IT-süsteemi hoitavat teavet hallatakse asjakohasel infoturbe tasemel, peab Atea töötaja märkima konkreetselt kõik failid, dokumendid või e-kirjad, mis sisaldavad teavet vastavalt selle tundlikkuse astmele, et teabe saaja oleks sellest teadlik. Märgistus peab vastama Atea andmete klassifitseerimise standarditele.

Atea andmete klassifitseerimise standardid koosnevad viiest tasandist, mille kohaselt järjestatakse e-kirjas või failis salvestatud teave kõige vähem tundlikust kõige rohkem tundliku teabeni. Klassifitseerimise standardid on sisse ehitatud Atea Microsoft Outlooki ja Wordi/Exceli/Powerpointi versioonidesse. Atea töötaja saab automaatselt märkida e-kirja, dokumendi või faili õige andmete klassifitseerimise märgistusega, valides tarkvaraprogrammi päisest vastava nupu.

Viis tasandit on järgmised:

1. äritegevusega mitte seotud: eraisikute vahelised e-kirja vestlused ja dokumendid, mis ei ole Ateaga seotud;

2. avalik: Ateat puudutav teave, mida võib avalikult levitada;

3. ettevõttesisene: teavet, mida võib vabalt levitada ettevõttesiseselt ja Atea äriüksustes ja 3.osapoole tarnijate juures. Ei ole mõeldud levitamiseks väljaspool Ateat või tema lepingulistele osapooltele;

4. konfidentsiaalne: teave, mille saaja peaks enda teada jätma ja mida ei tohi ilma teabeomanikuga kooskõlastamata jagada. Siia kuuluvad isikuandmed, mis tuleks eraldi märgistada. Isikuandmeid saab märgistada, kui teha konfidentsiaalset nuppu kasutades valik rippmenüül;

5. rangelt konfidentsiaalne: teave, mille omavolilisel avalikustamisel oleksid Ateale väga olulised negatiivsed tagajärjed. Sellist teavet tuleks säilitada krüptitud vormingus ja seda ei tohi ilma teabeomanikuga kooskõlastamata jagada. Sisaldab järgmist:

- tundlikud isikuandmed: vastavalt isikuandmete kaitse üldmäärusele tuleb teatavat liiki isikuandmeid käsitleda eriti turvalisi ettevaatusabinõusid rakendades. Sellised andmed on seotud järgmisega: etniline päritolu, poliitilised vaated, usulised veendumused, ametiühingute liikmesus ning geneetilised või biomeetrilised andmed. Tundlikud isikuandmed tuleks eraldi märgistada. Märgistamiseks teha rangelt konfidentsiaalset nuppu kasutades valik rippmenüül;

- hinnatundlik äriteave: selleks on salajane äriteave, näiteks võtmeklientide või varustajate andmed ning kaubandustingimused. See hõlmab ka teavet, mille kohta on kliendi või äripartneriga sõlmitud mitteavalikustamis- või konfidentsiaalsusleping. Viimaseks – selleks võivad olla ka ülimalt tundlikud intellektuaalomandi õigused, näiteks ärikontseptsioonid, ning ettevõtte siseselt välja töötatud tarkvara, meetodid ja vahendid;

- hinnatundlik teave: tegemist on konfidentsiaalse teabe eriliigiga, mis võib mõjutada Atea aktsiate hinda. See hõlmab olulisi finantsandmeid, mida ei ole veel avaldatud, või väga mahukate kliendi- või kaubalepingutega seotud konfidentsiaalsete läbirääkimiste seis.

- Atea kontserni finantsjuhti tuleb kohe teavitada kõigist töötajatest, kelle valduses on hinnatundlikku teavet. Need töötajad registreeritakse Atea kasutatavas Computershare'i siseringitehingute haldamise süsteemis CIMS. Rohkem teavet hinnatundliku teabega seotud vastavusmenetlustest leiab toimimisjuhendist.

Atea andmete klassifitseerimise standardite ja dokumentide märgistamise ja krüpteerimise ning e-posti teel edastamise korra täielik kirjeldus on saadaval teie riigi intraneti globaalse infoturbe veebilehel.

Isikuandmete haldamine
Vastavalt isikuandmete kaitse üldmäärusele on Ateal spetsiaalsed juriidilised kohustused

seoses isikuandmete käsitlemisega, kusjuures isikuandmeid määratletakse kui mis tahes teavet, mis viitab konkreetsele ja tuvastatavale isikule. Nende juriidiliste kohustuste kohaselt peab Atea dokumenteerima, et on võtnud piisavaid tehnilisi ja korralduslikke meetmed isikuandmete kaitse üldmääruse nõuete täitmiseks. Protsessi dokumentatsioon peab taotluse korral olema riigiasutustele kättesaadav.

Enne, kui Atea saab isikuandmeid koguma hakata, peab infoturbe juht olema täielikult dokumenteerinud ja üle vaadanud äriprotsessi, mida kasutades isikuandmeid käsitlema hakatakse. Iga funktsiooni andmekaitse haldur vastutab selle eest, et kõik isikuandmete käsitlemise protsessid oma funktsiooni piires oleksid dokumenteeritud ja ajakohastatud vastavalt isikuandmete kaitse üldmäärusele.

Dokumentatsioon peab tõendama, et Atea on võtnud piisavalt tehnilisi ja korralduslikke meetmeid, et täita isiku õigust oma isikuandmetele, ennetada ja vähendada andmetega seotud rikkumise mõju ning isikuandmetega seotud rikkumise korral seadusega kooskõlas reageerida. Isikuandmete kogumise protsessid peavad hõlmama ka andmete minimeerimise menetlust, st isikuandmete kustutamist, kui Atea neid enam ei vaja.

Isikuandmete kogumisel peab Atea isikut teavitama või saama temalt nõusoleku isikuandmete kogumiseks ja kasutamiseks. Isiku teavitamisel või temalt nõusoleku hankimisel peab Atea vastavalt isikuandmete kaitse üldmäärusele edastama järgmise teabe:

1. kogutavate ja töödeldavate isikuandmete kategooriad;
2. andmetöötluse eesmärk ja õiguslik alus;
3. isikuandmete saajad või nende vastuvõtjate kategooriad;
4. ajavahemik, mille jooksul andmeid kasutatakse, või kriteeriumid selle perioodi määratlemiseks;
5. isikuandme õigused oma isikuandmetele – sealhulgas õigus võtta nõusolek tagasi ja õigus andmetele juurdepääsule, nende kustutamiseks ja parandamiseks.
6. Isiku õigus esitada kaebus järelevalveasutusele.
7. Vajaduse korral edastatakse teade andmete edastamise kohta teise riiki ja kinnitus selle kohta, et andmete töötlemine teises riigis toimub kooskõlas isikuandmete kaitse üldmääruse sätetega andmekaitse piisavuse kohta.
8. Tundlike isikuandmete kogumisel peab Atea taotlema ja saama selgesõnalise nõusoleku isikult, kelle andmeid töödeldakse.

Isikuandmete kogumist käsitleva standardse privaatsusteate leiate oma riigi intraneti globaalse infoturbe veebilehelt.

Ateal on isikuandmete kaitse üldmääruse alusel erilised kohustused isikuandmetega seotud rikkumise korral. Andmetega seotud rikkumine on infoturbe vahejuhtum, mille tagajärjel saavad volitamata isikud juurdepääsu andmetele või põhjustavad andmete ebaseadusliku või juhusliku kaotsimineku.

Andmetega seotud rikkumise korral peaks Atea töötaja viivitamatult teavitama oma riigi või ühise teenindusüksuse infoturbe juhti. Infoturbe juht uurib andmetega seotud rikkumist koos Atea infoturbe korraldusega ja võtab vajalikke parandusmeetmeid, et teatada andmetega seotud rikkumisega tekitatud kahjust ja seda leevendada.

Kui andmetega seotud rikkumine puudutab isikuandmeid ja sellega kaasneb isikule kahju tekkimise oht, peab Atea rikkumise toimumise järel 72 tunni jooksul teavitama selle riigi järelevalveasutust, kus rikkumine toimus. Teates tuleb kirjeldada rikkumise laadi ja see peab sisaldama kokkuvõtet seotud andmesubjektidest ja kirjetest, rikkumise tõenäolisi tagajärgi ning võetavaid meetmeid.

Teavitada tuleb ka isikut, kelle isikuandmetega seoses rikkumine toime pandi, kui suur on sellele isikule kahju tekkimise oht. Kui isikut ei ole võimalik individuaalselt teavitada, piisab ka avalikust teadaandmisest.

Kliendilepingud

Atea haldab paljude klientide jaoks andmetaristut ja rakendusi kas kliendi juures kohapeal või oma andmekeskuse kaudu. Nendel juhtudel vastutab Atea kliendi andmete töötlemise eest lepingulise kohustuse eest ning tal on isikuandmete kaitse üldmääruse kohaselt juriidiline kohustus tagada, et see kaitseb nõuetekohaselt iga isiku isikuandmete privaatsuse õigusi, kelle isikuandmed sisalduvad kliendi andmetes.

Isikuandmete kaitse üldmääruse järgimiseks peab Atea kliendiandmete infrastruktuuri ja rakenduste haldamisel olema oma klientidega töötlemise leping (DPA). Andmetöötlusleping peab dokumenteerima Atea poolt kliendi juhiste alusel teostatavate andmetöötlustoimingute ulatuse, laadi ja

kestuse. See dokumentatsioon peab sisaldama ka kokkuvõtet sellest, millist tüüpi isikuandmeid Atea kliendi nimel töötleb ja milliste isikute kategooriate isikuandmeid töödeldakse.

DPA peab sisaldama järgmist kinnitust Atealt vastavalt isikuandmete kaitse üldmäärusele:

1. Atea töötleb isikuandmeid ainult kliendi dokumenteeritud juhiste alusel ja järgib andmekaitseseadusi
2. Atea töötaja, kes töötleb kliendi jaoks isikuandmeid, peab olema endale võtnud konfidentsiaalsuskohustuse. Atea ei määra kliendi loata alltöövõtjaid isikuandmete töötlemiseks kliendi jaoks.
3. Atea on võtnud piisavalt tehnilisi ja korralduslikke meetmeid, et tagada kliendiga kokkulepitud turvalisuse tase vastavalt töödeldavate andmete riskile.
4. Atea on võtnud piisavalt meetmeid, et täita oma juriidilisi kohustusi isikute õiguste suhtes kontrollida oma andmete töötlemist nagu on kirjeldatud isikuandmete kaitse üldmääruses
5. Atea annab kliendile kogu vajaliku teabe, et näidata oma vastavust isikuandmete kaitse üldmääruse andmetega seotud eraelu puutumatuse kohustustele ja osaleda kliendi nõuetele vastavuse kontrollis, kui seda nõutakse.
6. Atea teavitab klienti isikuandmetega seotud rikkumisest põhjendamatu viivituseta
7. Atea kustutab või tagastab kliendile kõik isiklikud andmed teeninduslepingu lõpus

Kui Atea kasutab kliendiga seotud andmetöötluskohustuste täitmiseks väliseid alltöövõtjaid (nt kolmanda osapoole pilveteenused, konsultandid või infrastruktuuri pakkujad), peab Atea'l olema nende alltöövõtjatega eraldi DPA, kus alltöövõtja annab sarnase kinnituse ülaltoodud avaldused.

Ateal on standardne DPA, mida soovitatakse kasutada koos kõigi klientide ja alltöövõtjatega. Andmekaitselepingu leiate oma riigi intraneti globaalse infoturbe veebilehelt. Iga riigi infoturbe juht vastab DPAd puudutavatele küsimustele ja saab pakkuda abi teenuseosutajalt allkirjastatud DPA hankimise protsessis.

Kliendi andmetega seotud isikuandmetega seotud rikkumise korral peab Atea teavitama klienti viivitamatult andmetega seotud rikkumisest teadasaamisest. Seejärel peab Atea tegema koostööd oma kliendiga ja võtma mõistlikke samme tagamaks, et klient suudab täita oma kohustused teatada rikkumisest tulenevatest rikkumistest, ning teha parandusmeetmeid rikkumisega tekitatud kahju leevendamiseks.

Olulised punktid:

Süsteemi registreerimine

Kõik Ateas kasutatavad IT-süsteemid tuleb registreerida infoturbe juhi juures selles riigis või äriüksuses, kus süsteemi kasutatakse. See hõlmab pilveteenuseid, mida ostetakse liitumiste kaudu ja hallatakse väljaspool Ateat.

Infoturbeametnik kontrollib IT-süsteemi, et kinnitada, et see vastab Atea IT-turvastandarditele enne süsteemi kasutamiseks heakskiitmist. Kui süsteem on registreeritud, määratakse süsteemi omanik. Süsteemi omaniku roll on tagada, et süsteemi kasutatakse vastavalt Atea andmekaitsepoliitikale, pöörates erilist tähelepanu juurdepääsuõiguste haldamisele.

Andmete klassifitseerimine

Et tagada, et väljaspool volitatud IT-süsteemi hoitavat teavet hallatakse asjakohase infoturbe tasemega, peab Atea töötaja märkima konkreetselt kõik failid, dokumendid või e-kirjad, mis sisaldavad teavet vastavalt selle tundlikkusele nii, et seda mõistaksid kõik saajad. Märgistus peab vastama Atea andmete klassifitseerimise standarditele.

Kõiki isikuandmete käitlemise tavasid peab dokumenteerima ja seda kontrollima ka infoturbe juht. Kõigile Atea juhtidele on määratud andmekaitse haldur, kes vastutab oma riigis (või ühises teenindusüksuses) konkreetse ärifunktsiooni eest. Andmekaitse halduri roll on kontrollida, kas kõik funktsiooni äriprotsessid vastavad Atea andmekaitse põhimõtetele kooskõlas isikuandmete kaitse üldmäärusega.

Isikuandmete haldamine

Isikuandmete kogumisel peab Atea teavitama isikut või saama tema nõusoleku, et nende isikuandmeid kogutakse ja kasutatakse vastavalt isikuandmete kaitse üldmäärusele. Isikuandmete kaitse üldmäärusel on mitmeid teabenõudeid, mis on seotud teate sisuga (vt põhiteksti).

Andmetega seotud rikkumine on infoturbe vahejuhtum, mille tagajärjel saavad volitamata isikud juurdepääsu andmetele või põhjustavad andmete ebaseadusliku või juhusliku kaotsimineku. Ateal on isikuandmete kaitse üldmääruse alusel erilised kohustused isikuandmetega seotud rikkumise korral.

Andmete rikkumise kahtluse korral peaks Atea töötaja viivitamatult teavitama oma riigi infoturbe juhti või jagatud teenindusüksust. Alternatiivselt võib saata e-kirja aadressile infosec@atea.com, kuhu laekuvad e-kirjad edastatakse kõik otse Atea kontserni infoturbe juhile.

Isikuandmete kaitse üldmääruse järgimiseks peab Atea kliendiandmete infrastruktuuri ja rakenduste haldamisel olema oma klientidega töötlemise leping (DPA). Ateal peab olema ka oma allhankijate või müüjatega DPA, kes töötleb andmeid Atea nimel või nimel. Isikuandmete kaitse üldmäärusel on arvukad andmekaitseasutuse sisuga seotud teavitamisnõuded (vt põhiteksti).

4. IT INFRASTRUKTUURI TURVALISUS – VÕIMALIKUD TEGEVUSED KÕIGILE TÖÖTAJATELE

Atea IT-infrastruktuur koosneb kõigist riist-, tarkvara ja võrgukomponentidest, mis toetavad ärisüsteemide ja IT-toega protsesside kasutajatele edastamist. Andmekaitse Ateas sõltub kõikidest töötajatest, kes kasutavad vastutustundlikult Atea IT-infrastruktuuri varasid.

Järgmised eeskirjad on seotud kõigi Atea töötajatega, kes on Atea IT-infrastruktuuri kasutajad, ning katavad seadme turvalisuse, süsteemi juurdepääsu, failide salvestamise, võrgu turvalisuse, side ja füüsilise turvalisuse. Lisaks peavad töötajad, kes vastutavad Atea IT-operatsioonide juhtimise eest, võtma eraldi ja ulatuslikumaid infotehnoloogia turvalisuse alase koolituse, mis vastab nende ülesannetele.

Seadme turvalisus:
Atea töötaja peab oma töövahendite, näiteks arvutite, tahvelarvutite ja nutitelefonide abil kasutama turvameetmeid. Need seadmed on kalduvad varguse, pahavara ja volitamata kasutamise vastu. Atea arvutid, tahvelarvutid ja nutitelefonid tuleb alati jälgida või salvestada turvalises kohas. Kui neid seadmeid ei kasutata, tuleb need lukustada PIN/parooli kaitsega või sulgeda.

Kõikidel Atea arvutitel, tahvelarvutitel ja nutitelefonidel peaks olema installitud krüpteerimislahendused, et vältida volitamata juurdepääsu kõvakettale. Atea Windows-arvutid aktiveeritakse Bitlockeri krüpteerimislahendusega. Apple Maci mudelite puhul on sisseehitatud funktsioon kõvaketta krüpteerimiseks, mis tuleb kasutamisel aktiveerida. Kõik iPhone'i ja iPadi seadmed on eelnevalt krüpteeritud. Krüpteerimine peab Android mobiiltelefonidel ja tablettidel olema käsitsi lubatud. Krüpteerimine peaks olema aktiveeritud ka eemaldatavas mälus, näiteks USB-seadmetes, mida on lihtne kaotada. Töötajad, kes otsivad toetust oma töövahendite krüptimiseks, võivad pöörduda Atea teenindustoe poole.

Atea töötaja ei tohiks alla laadida tarkvara oma arvutisse, mis ei ole pärit Atea IT-osakonnast. Atea IT-osakond pakub Acceleratori portaali kaudu erinevaid tarkvararakendusi. Neid rakendusi ajakohastatakse regulaarselt, et säilitada õige turvalisuse tase. Kui Atea töötaja peab oma arvutisse laadima välise tarkvara, mis ei kuulu kiirendusportaali, peaksid nad kõigepealt saama oma juhilt ja kohalikult IT-organisatsioonilt heakskiidu.

Atea arvutid on eelinstallitud pahavaravastase ja tulemüüri rakendustega. Kui teil on mingeid kahtlusi teie pahavaravastase kaitse kohta, võtke ühendust Atea teenindustoega. Kui teile saadetakse pahavaravastase programmi hoiatus või kui teie arvuti toimib ebanormaalselt, võib see olla märk sellest, et teie arvuti on ohustatud. Arvutil esinevate pahavara märkide hulka võivad kuuluda sagedane külmutamine või ebatavaliselt aeglane töötlemine või toimingud, mis toimuvad ilma algatamiseta, sealhulgas hüpikaknad või muud ekraanil tehtavad muudatused.

Kui kahtlustate, et teie arvuti on kahjustatud, lõpetage koheselt töö arvutiga ning ühendage arvuti võrgust välja. Seejärel võtke ühendust Atea Servicedesk'iga ja andke teavet selle kohta, millised sümptomid on tekitanud kahtlust, et arvuti on rünnatud pahavaraga ja millised sündmused võisid põhjustada arvuti kahjustamist.

Kõik kasutusest kõrvaldatavad töövahendid tuleb kustutada kõikidest andmetest enne, kui need Atea kontorist saadetakse hoolduseks, ringlussevõtuks või taaskasutamiseks. Seda tuleks teha kooskõlas igas riigis rakendatavate IT-menetlustega. Need toimingud leiate teie riigi sisevõrgu veebisaidilt Global Information Security.

Süsteemile juurdepääs:
Atea töötajale tuleks anda juurdepääs süsteemidele ainult siis, kui see on nende töö jaoks vajalik. Süsteemide kasutamise õigusi tuleb pidevalt kontrollida, et tagada selle poliitika säilitamine ja juurdepääs lõpetatakse niipea, kui seda enam ei vajata. Kui Atea töötajal on juurdepääs süsteemidele, mida nad enam ei vaja, peaksid nad oma kasutusõiguste lõpetamiseks viivitamatult võtma ühendust süsteemiomanikuga.

Kui süsteemile juurdepääsu õigused antakse Atea töötajale, tuleb kasutajatunnus ja ajutine parool jaotada eraldi. Ajutine parool tuleb pärast esimest sisselogimist viivitamatult muuta ja seda ei tohi kirjutada ega ühiskasutada ühegi inimesega. Töötajad ei tohi anda teistele kasutajatele juurdepääsuõigusi.

Failide säilitamine:
Kõik Atea töötajad vastutavad oma töötailide (nt MS Wordi/Exceli/Powerpointi failide) turvalise haldamise eest. Kõik failitüübid tuleks salvestada Atea sisemistesse jagatud failiserveritesse, OneDrive'i kontodesse või Sharepointi keskkonda. Muid väliseid salvestuskohti, sealhulgas Dropboxi või Google Drive'i, ei tohi kasutada Atea failide salvestamiseks ilma riigi IT-osakonna selgesõnalise loata, kuna Atea ei suuda tagada nende säilitamiskohtade turvalisust. Atea töötaja ei tohi salvestada ettevõtte andmeid oma seadmete kõvaketastele, kuna nad ei ole automaatselt varundatud ja seetõttu on andmete kadumise oht.

Failid tuleb märgistada vastavalt Atea andmete klassifitseerimise normidele (5 taset). Rangelt konfidentsiaalseks märgistatud failid tuleb salvestada krüpteeritud kujul. Isikuandmeid sisaldavad failid tuleb samuti märgistada ja säilitada vastavalt isikuandmete kaitse üldmäärusele.

Atea töötaja peab isikuandmete salvestamisel failidesse olema väga ettevaatlik, kuna isikuandmete kaitse üldmääruse andmekaitse nõuded on ranged. Töötajad ei tohi kasutada isikuandmeid failides väljaspool algset eesmärki, mis oli määratletud ja edastatud isikule, kelle andmeid koguti. Töötajad peavad piirama isikuandmeid sisaldavate failide jagamist, et vältida nende andmetega seotud rikkumist või väärkasutamist ning kustutada isikuandmed niipea, kui seda enam ei vajata. See kehtib kõigi failide kohta, mis on loodud Atea töötaja poolt, sealhulgas MS Wordi/Exceli/Powerpointi failid.

Võrgu turvalisus:
Ainult Atea kliendid (arvutid mis on konfigureeritud vastavalt Atea standardile) ühendatakse Atea domeeni. Atea mobiilseadmed peavad ühenduma ainult Atea mobiilseadmete Wi-Fi võrguga. Teiste arvutite või mobiilseadmete puhul kasutatakse Atea külalistele mõeldud Wi-Fi võrku.

Atea pakub mitte kontoris olevate töötajatele võimalust ühenduda sisevõrguga sisevõrguga Cisco VPN või Citrixi kaudu. See võimaldab juurdepääsu nii ühisele failisüsteemile kui ka ühistele ärirakendustele. Ühendamine Cisco VPN-iga eeldab, et arvuti kuulub Ateale ja on Atea domeeni (ONE) liige ja et arvutisse on paigaldatud pahavaravastane tarkvara.

Atea töötaja ei tohi kunagi kliendi võrguga ühenduda ilma kliendi eelneva nõusolekuta, kui kliendilepingus ei ole sätestatud teisiti. Kliendiga tuleb ühendust võtta iga kord, kui Atea töötaja oma soovib ühenduda kliendi võrku ja Atea töötaja peab alati teavitama klienti, milliseid tegevusi on ta teinud kliendi võrgus.

Atea töötaja peab reisimisel kasutama avalikke Wi-Fi-võrke ettevaatlikult. Andmete liikumist avalike võrkude kaudu võidakse jälgida või kuulata pealt. Enne Wi-Fi-võrgu kasutamist peab Atea töötaja veenduma, et võrk on turvaline ja õigustatud ning usaldusväärselt pakkujalt. Kui on põhjust kahelda avaliku Wi-Fi-võrgu turvalisuses, peab Atea töötaja kasutama mobiilsidevõrku. Atea Teenindus vajadusel pakub tuge arvuti ühendamiseks mobiilsidevõrguga.

Eeldatakse, et Atea töötaja kasutab Internetti oma igapäevatöös. Isiklik sirvimine on lubatud, kuid see peaks piirduma saitidega, mille sisu sobib töökohale. Online-mängud või hasartmängud ei ole lubatud ning failide jagamine või meedia voogesitus Interneti kaudu peaks piirduma tööga seotud sisuga. Kõik töötajad peaksid teadma, et Atea analüüsib interneti liiklust Atea vastu suunatud rünnakute tuvastamiseks ning selle jälgimisega on võimalik ka tuvastada ebakorrektne interneti kasutamine.

Interneti lehekülgedele pääsemisel olge ettevaatlik, et veebileht oleks korrektne - eriti kui te olete teisele lehele ümber suunanud. Ärge kunagi klikkige veebilehtedel olevatel linkidel või hüpikakendel, kui need näivad kahtlasted, kuna need võivad sisaldada pahavara, mida saab teie seadmesse laadida.

Side (e-post/sotsiaalmeedia):
E-post on kriitiline digitaalse kommunikatsiooni vahend Atea töötajale. See on infoturbe peamine haavatusse allikas, sest see annab ründajatele võimaluse suunata Ateale pahavara ja muid ohte madala hinnaga ja madala süüdistuse esitamise riskiga.

Üks sageli Atea vastu toime pandav identiteedipettus (andmepüük) on olukord, kus ründaja võtab Atea töötajaga otse e-posti kaudu ühendust. E-kiri on pealtnäha usaldusväärsest allikast; sageli kasutatakse valesid isikuandmeid, näiteks mõne teise Atea töötaja, äripartneri või sellise tarnija nagu tehnoloogiaettevõtte või panga andmeid. E-kirjaga üritatakse Atea töötajat veenda vastama, näiteks kandma üle raha, avaldama sisselogimise / salasõna andmed või muud tundlikku teavet või klõpsama lingil või manusel,

mis laadib kasutaja arvutisse või mobiiltelefoni kahjuliku tarkvara (nn pahavara).

E-kiri, manus või link on pealtnäha ohutu – näiteks võib see olla maskeeritud kui kolleegi saadetud e-kiri, pakkumine/arve tarnijalt või teavitus selliselt pilvekontolt nagu OneDrive. Seetõttu peavad Atea töötajad olema äärmiselt valvsad e-posti ja muu teabevahetusega seotud võimalike pettuste suhtes – ka siis, kui sõnum tundub olevat usaldusväärsest allikast.

Atea töötajad ei tohiks kunagi avada oma seadmes linke või manuseid, kui nad kahtlevad e-kirja või teavituse õiguspärasuses. Kui Atea töötajal peaks olema kahtlusi e-kirja õiguspärasuse suhtes või kui ta on kogemata kahtlase lingi või manuse avamisega vastanud võimalikule pettusekatsele, peaks ta võtma kohe ühendust Atea teenindustoega ja probleemist teada andma.

Sageli rünnatakse töötajate e-posti kontosid eesmärgiga saada ligipääsu töötaja tundlikele ärifailidele. Seetõttu ei tohiks e-posti kasutada olulise äriinformatsiooni arhiveerimiseks. Ärialast teavet tuleks säilitada või levitada kasutades turvalisi ärisüsteemide või failide jagamise keskkondi ning mitte kasutada selleks e-posti.

E-posti isiklik kasutamine on lubatud tingimusel, et kasutamine ei ole vastuolus Atea ärihuvidega ega takista töö tegemist. Privaatne e-kirjavahetus peab alati olema töökohale sobiv ja see peaks olema tähistatud “Non-business”. Lisaks ei tohiks ettevõtte e-posti konto kasutamine isiklikus suhtlemises jätta muljet, et kirjavahetus on seotud Atea teenustega või on Atea poolt heaks kiidetud.

Sotsiaalmeedia on samuti Atea töötaja jaoks sagedane suhtlusvahend. Õigesti kasutatuna annab sotsiaalmeedia Atea töötajale võimaluse omandada ja edastada teadmisi, luua ärisuhteid ja tugevdada Atea kaubamärki. Teisest küljest võib sotsiaalmeedia olla Ateale ja selle töötajatele ebasoodsa kasutuse korral või tundlikku info levitamise tõttu väga kahjulik.

Seetõttu peaks Atea töötaja olema väga ettevaatlik, millist teavet ta sotsiaalmeedias jagab. Isikuandmeid (sealhulgas nimesid, fotosid jne) saab jagada ainult Atea äritegevusega seotud sotsiaalmeedia postitustega, kui isik, kelle andmeid jagatakse, nõustub sellega.

Büroo turvalisus:

Atea töötaja peab identifitseerimiseks kandma turvamärke. Kõik Atea külalised peavad registreeruma vastuvõtulauas ning olema varustatud külalismärgiga, mis peaks olema nähtavalt kantud. Külastajaid tuleb vastu võtta vastuvõtu laua juures ning visiidi lõpus tuleb külastaja saata vastuvõtu laua juurde, et tagastada märgistus. Külastajaid ei tohi jätta üksi Atea ruumidesse.

Kogu tundlik teave mida pole vaja enam kasutada tuleb laudadelt eemaldada paigaldades nad turvalisse kohta. Koosolekute lõpus tuleb puhastada ära kõik tahvlid. Konfidentsiaalsed dokumendid mis pole enam vajalikud tuleb hävitada dokumendipurustajates või visata spetsiaalsetesse konteineritesse.

KÕIGE OLULISEM - IT infrastruktuuri turvalisus

Seadme turvalisus:
Kõikidel Atea arvutitel, tahvelarvutitel ja nutitelefonidel peaks olema installitud krüpteerimislahendused, et vältida volitamata juurdepääsu kõvakettale. Atea arvutid, tahvelarvutid ja nutitelefonid tuleb alati jälgida või salvestada turvalises kohas. Kui neid seadmeid ei kasutata, tuleb need lukustada PIN/parooli kaitsega või sulgeda.

Atea töötaja ei tohiks alla laadida tarkvara oma arvutisse, mis ei ole pärit Atea IT-osakonnast. Kui Atea töötaja peab oma arvutisse laadima välise tarkvara, mis ei kuulu kiirendusportaali, peaksid nad kõigepealt saama oma juhilt ja kohalikult IT-organisatsioonilt heakskiidu.

Atea arvutid on eelinstallitud pahavaravastase ja tulemüüri rakendustega. Kui teil on mingeid kahtlusi teie pahavaravastase kaitse kohta, võtke ühendust Atea teenindustoega.

Kui kahtlustate, et teie arvuti on nakatunud pahavaraga või kahjustatud, lõpetage koheselt töö arvutiga ning ühendage arvuti võrgust välja. Seejärel võtke ühendust Atea teenindustoega.

Süsteemile juurdepääs:
Atea töötajale tuleks anda juurdepääs süsteemidele ainult siis, kui see on nende töö jaoks vajalik. Süsteemide kasutamise õigusi tuleb pidevalt kontrollida, et tagada selle poliitika säilitamine ja juurdepääs lõpetatakse niipea, kui seda enam ei vajata.

Failide säilitamine:
Kõik Atea töötajad vastutavad oma tööfailide (nt MS Wordi/Exceli/Powerpointi failide) turvalise haldamise eest. Failid tuleb märgistada vastavalt Atea andmete klassifitseerimise normidele (5 taset). Isiklikku teavet sisaldavad failid tuleb eraldi märgistada. Rangelt konfidentsiaalseks märgistatud failid tuleb salvestada krüpteeritud kujul.

Kõik failitüübid tuleks salvestada Atea sisemistesse jagatud failiserveritesse, OneDrive'i kontodesse või Sharepointi keskkonda. Muid väliseid salvestuskohti, sealhulgas Dropboxi või Google Drive'i, ei tohi kasutada Atea failide salvestamiseks ilma riigi IT-osakonna selgesõnalise loata, kuna Atea ei suuda tagada nende säilitamiskohtade turvalisust Atea töötaja ei tohi salvestada ettevõtte andmeid oma seadmete kõvaketastele, kuna nad ei ole automaatselt varundatud ja seetõttu on andmete kadumise oht.

Võrgu turvalisus:
Ainult Atea kliendid (arvutid mis on konfigureeritud vastavalt Atea standardile) ühendatakse Atea domeeni. Atea mobiilseadmed peavad ühenduma ainult Atea mobiilseadmete Wi-Fi võrguga. Teiste arvutite või mobiilseadmete puhul kasutatakse Atea külalistele mõeldud Wi-Fi võrku.

Enne Wi-Fi-võrgu kasutamist peab Atea töötaja veenduma, et võrk on turvaline ja õigustatud ning usaldusväärselt pakkujalt

Juurdepääs internetile töövahendist peaks piirduma saitidega, mille sisu sobib töökohale. Kõik töötajad peaksid teadma, et Atea analüüsib interneti kaudu liiklust Atea vastu suunatud rünnakute tuvastamiseks ning see jälgib ka Interneti valesti kasutamist.

Veebilehekülgedele pääsemisel olge ettevaatlik, et veebileht on täpne - eriti siis, kui olete teiselt leheküljelt ümber suunatud. Ärge kunagi klikkige veebilehtedel olevatel linkidel või hüpikakendel, kui need näivad kahtlased, kuna need võivad sisaldada pahavara, mida saab teie seadmesse laadida.

Side (e-post/sotsiaalmeedia):
E-post on infoturbe peamine haavatusse allikas, sest see annab ründajatele võimaluse suunata Ateale pahavara ja muid ohte madala hinnaga ja madala süüdistuse esitamise riskiga.

Üks sageli Atea vastu toime pandav identiteedipettus (andmepüük) on olukord, kus ründaja võtab Atea töötajaga otse e-posti kaudu ühendust. E-kiri on pealtnäha usaldusväärsest allikast; sageli kasutatakse valesid isikuandmeid, näiteks mõne teise Atea töötaja, äripartneri või sellise tarnija nagu tehnoloogiaettevõtte või panga andmeid. E-kirjaga üritatakse Atea töötajat veenda vastama, näiteks kandma üle raha, avaldama sisselogimise / salasõna andmed või muud tundlikku teavet või klõpsama lingil või manusel, mis laadib kasutaja arvutisse või mobiiltelefoni kahjuliku tarkvara (nn pahavara).

Atea töötajad ei tohiks kunagi avada oma seadmes linke või manuseid, kui nad kahtlevad e-kirja või teavituse õiguspärasuses. Kui Atea töötajal peaks olema kahtlusi e-kirja õiguspärasuse suhtes või kui ta on kogemata kahtlase lingi või manuse avamisega vastanud võimalikule pettusekatsele, peaks ta võtma kohe ühendust Atea teenindustoega ja probleemist teada andma.

E-posti isiklik kasutamine on lubatud tingimusel, et kasutamine ei ole vastuolus Atea ärihuvidega ega takista töö tegemist. Privaatne e-kirjavahetus peab alati olema töökohale sobiv ja see peaks olema tähistatud kui "Non-business".

Atea töötaja peaks olema äärmiselt ettevaatlik, millist teavet nad jagavad sotsiaalmeedias seoses Ateaga. Isikuandmeid (sealhulgas nimesid, fotosid jne) saab jagada ainult Atea äritegevusega seotud sotsiaalmeedia postitustega, kui isik, kelle andmeid jagatakse, nõustub sellega.

Büroo turvalisus:
Atea töötaja peab identifitseerimiseks kandma turvamärke. Kõik Atea külastajad peavad registreeruma vastuvõtulauas ning olema varustatud külalismärgiga, mis peaks olema nähtavalt kantud.

Kogu tundlik teave mida pole vaja enam kasutada tuleb laudadelt eemaldada paigaldades nad turvalisse kohta.

Valdusettevõte
Atea ASA
Atea ASA
Brynsalleen 2
Box 6472 Etterstad
NO-0605 Oslo
+47 22 09 50 00
Reg nr 920 237 126
investor@atea.com
atea.com

Norra
Atea AS
Brynsalleen 2
Box 6472 Etterstad
NO-0605 Oslo
+47 22 09 50 00
Reg nr 976 239 997
info@atea.no
atea.no

Rootsi
Atea AB
Kronborgsgränd 1
Box 18
SE-164 93 Kista
+46 (0)8 477 47 00
Reg nr 556448-0282
info@atea.se
atea.se

Taani
Atea A/S
Lautrupvang 6
DK-2750 Ballerup
+45 70 25 25 50
Reg nr 25511484
info@atea.dk
atea.dk

Soome
Atea Oy
Jaakonkatu 2
PL 39
FI-01621 Vantaa
+ 358 (0)10 613 611
Reg nr 091 9156-0
customercare@atea.fi
atea.fi

Leedu
Atea Baltic UAB
J. Rutkausko st. 6
LT-05132 Vilnius
+370 5 239 7899
Reg nr 300125003
info@atea.lt
atea.lt

Kontserni logistika
Atea Logistics AB
Smedjegatan 12
Box 159
SE-351 04 Växjö
+46 (0)470 77 16 00
Reg nr 556354-4690
customer.care@atea.se

Kontserni jagatud teenused
Atea Global Services SIA
Mukusalas Street 15
LV-1004 Riia
+371 67359600
Reg nr 50203101431
rigainfo@atea.com
ateaglobal.com

ATEA