TP2B THE PLACE TO BE

ATEA

TIETOTURVARISKIEN HALLINTA: KÄYTÄNTÖJÄ TYÖNTEKIJÖILLE

Versio 1.0 - julkaistu huhtikuussa 2019

TOIMITUSJOHTAJAN VIESTI

Atean missiona on rakentaa tulevaisuutta tietotekniikalla.

Uskomme, että tietotekniikka yhdessä tiedon ja luovuuden kanssa voi parantaa tuottavuutta ja elintasoa kaikkialla yhteiskunnassa. Tuemme yrityksiä ja julkisen sektorin organisaatioita kehittämällä digitaalisia ratkaisuja, joiden avulla saadaan aikaan enemmän – tehokkaammin ja pienemmillä resursseilla.

Samalla ymmärrämme, mitä riskejä liittyy teknologioihin, jotka tallentavat ja käsittelevät yhä suurempia tietomääriä. Kun organisaatiot käsittelevät enemmän tietoja ja automatisoivat prosesseja tietotekniikkajärjestelmiensä ja -verkkojensa kautta, myös tietovarkauksien, identiteettipetosten ja kyberhyökkäyksien aiheuttamien toimintahäiriöiden riski kasvaa. Tietomurto voi myös johtaa siihen, että henkilön tietoja käytetään ilman hänen suostumustaan. Tietojen väärinkäytöllä voidaan aiheuttaa vahinkoa ja loukata oikeutta yksityisyyteen.

Pohjoismaiden ja Baltian johtavana tietotekniikan tarjoajana Atealla on erityinen vastuu huolehtia siitä, että yrityksen toiminta täyttää tietoturvallisuuden tiukat standardit. Atea suunnittelee, ottaa käyttöön ja hoitaa IT-infrastruktuuriratkaisuja alueemme suurimmissa ja tärkeimmissä organisaatioissa. Suurin osa liikevaihdostamme on peräisin julkishallinnon asiakkailta. Joukossa on asiakkaita, joiden tietojenkäsittely on äärimmäisen luottamuksellista, esimerkiksi puolustusvoimat ja poliisi. Tarjoamme myös työn kannalta olennaisia IT-ratkaisuja alueemme suurimmille yrityksille.

Tämä asiakirja on opas tietoturvariskien hallitsemiseen Atealla. Se tarjoaa yleiskuvan keskeisistä turvallisuusriskeistä, tietosuojakäytännöistä ja hallintomenettelyistä, jotka vaikuttavat kaikkiin yrityksessämme työskenteleviin. Työntekijöiden, joilla on erityinen vastuu IT-toiminnasta ja järjestelmien valvonnasta, on suoritettava tehtäviensä mukaan erillisiä, laajempia testejä tietoturva- ja tietosuojakäytännöistä.

Dokumentaatio on jaettu neljään osioon, joiden tärkeimmät kohdat tiivistetään kunkin osion lopussa. Nämä neljä osiota ovat kuvattu yksityiskohtaisesti, sillä kyseessä on monimutkainen ja liiketoimintakriittinen aihe. On erityisen tärkeää, että työntekijät painavat mieleensä eri osioiden lopussa olevat kertaukset ja voivat tarvittaessa virkistää muistiaan näiden avulla.

Kaikkien Atean työntekijöiden odotetaan tutustuvan tämän asiakirjan sisältöön. Sen varmistamiseksi, että kaikki Atean työntekijät ovat ymmärtäneet asiakirjan sisällön, Code of Conductia koskevaan testiin on lisätty kymmenen tietoturvaa koskevaa kysymystä. Testi on pakollinen kaikille Atean työntekijöille. Työntekijöiden käytössä on verkkokoulutus, jonka avulla he voivat perehtyä tietoturvamenettelyihin ja valmistautua Code of Conduct-testiin.

Atea on suuri organisaatio, joka toimii seitsemässä maassa ja lähes 90 toimipisteessä. Konsernille ja jokaiseen maahan on nimetty oma tietoturvavastaava, joka tukee tietoturvamenettelyiden toimeenpanoa Atean organisaation eri osissa.

Steinar Sønsteby
Toimitusjohtaja

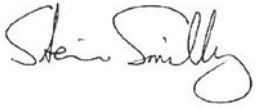
Jos sinulla on kysymyksiä tai huolenaiheita tietoturvasta Atealla, pyydämme sinua toimimaan seuraavasti:

- Jos epäilet, että tietokoneessasi on haittaohjelma tai haluat esittää yleisiä IT-turvallisuutta koskevia kysymyksiä, ota yhteyttä Atean palvelupisteeseen.
- Jos haluat ilmoittaa epäilyttävästä sähköpostista, huijausyrityksestä tai mistä tahansa muusta tapahtumasta, joka voi vaarantaa Atean tietoturvan, ota yhteyttä Atean palvelupisteeseen.
- Jos epäilet, että tietojärjestelmissä tai asiakirjoissa olevia henkilö- tai liiketoimintatietoja on paljastettu luvattomasti, ota yhteyttä sen maan tietoturvajohtajaan, jossa työskentelet. Voit myös lähettää sähköpostia suoraan osoitteeseen infosec@atea.com.

Jos haluat puhua suoraan Atea-konsernin tietoturvajohtajalle (CISO) tai oman maasi tietoturvajohtajalle, heidän nimensä löytyvät Atean Compliance-sivustolta: atea.com/trust. Osoitteeseen infosec@atea.com lähetetyt sähköpostiviestit välitetään suoraan Atea-konsernin tietoturvajohtajalle.

Otamme mielellämme vastaan kysymyksiä ja palautetta ja lupaamme, että ilmoittavalle taholle ei aiheudu haittaa ilmoituksen tekemisestä. Jos kuitenkin haluat ilmoittaa ongelmasta nimettömästi, voit lähettää raportin Whistleblower Hotline -palveluumme. Linkki Whistleblower Hotline -palveluun löytyy Atean Compliance-sivustolta: atea.com/trust. Whistleblower Hotline -palvelussa raportoidut asiat lähetetään riippumattomaan asianajotoimistoon, jossa ne käsitellään ja lähetään Atean organisaation asianmukaiselle tasolle.

Tietoturvan tiukkojen standardien ylläpitäminen on olennaista Atean liiketoiminnalle ja mahdollisuudellemme tehdä yhteistyötä asiakkaiden ja kumppaneiden kanssa alueemme tärkeimpien IT-haasteiden parissa. Kiitos Atean tietoturvamenettelyiden noudattamisesta ja siitä, että avullanne Atea voi olla The Place to Be.



Kertaus:

Atealle on ensiarvoisen tärkeää, että kaikki työntekijät pitävät yllä tietoturvan tiukkoja standardeja.

Konsernille ja jokaiseen maahan on nimetty oma tietoturvavastaava, joka tukee tietoturvamenettelyiden toimeenpanoa kaikissa Atea-organisaation osissa. Löydät tietoturvavastaavien nimet Atean Compliance-sivustosta: atea.com/trust.

Jos sinulla on kysymyksiä tai huolenaiheita tietoturvasta Atealla, pyydämme sinua toimimaan seuraavasti:

- Jos epäilet, että tietokoneessasi on haittaohjelma tai haluat esittää yleisiä IT-turvallisuutta koskevia kysymyksiä, ota yhteyttä Atean palvelupisteeseen.
- Jos haluat ilmoittaa epäilyttävästä sähköpostista, huijausyrityksestä tai mistä tahansa muusta tapahtumasta, joka voi vaarantaa Atean tietoturvan, ota yhteyttä Atean palvelupisteeseen.
- Jos epäilet, että tietojärjestelmissä tai asiakirjoissa olevia henkilö- tai liiketoimintatietoja on paljastettu luvattomasti, ota yhteyttä sen maan tietoturvajohtajaan, jossa työskentelet.
- Voit myös lähettää sähköpostia osoitteeseen infosec@atea.com. Viestisi välitetään suoraan Atea-konsernin tietoturvajohtajalle.

Sisältö

1. TIETOTURVA – YLEISKUVA JA RISKIENHALLINTA

Tieto on olennaisen tärkeää minkä tahansa organisaation toiminnan kannalta. Tietoturvallisuuden hallintajärjestelmä (information security management system, ISMS) on toimintatapojen, menettelyjen, työkalujen ja toimintojen joukko, jota organisaatio käyttää suojaamaan tietoa luvattomalta pääsyltä ja väärinkäytöltä.

ISMS:n luominen edellyttää sitä, että organisaatio tunnistaa omat tietovaransa. Tällä tarkoitetaan kaikkea organisaatiossa käsiteltyä tietoa sen muodosta riippumatta: digitaalista, kirjallista ja sanallista tietoa. Atealla tiedot jaetaan sisäiseen käyttöön tarkoitettuihin tietoihin sekä ulkoisiin tietoihin, joita Atea hallitsee ja käsittelee palveluna asiakkailleen.

Tietoturvallisuuden hallintajärjestelmän tarkoitus on suojata tietovaroja ja säilyttää niiden luottamuksellisuus, eheys ja saatavuus.

- Luottamuksellisuus tarkoittaa sitä, että tiedot ovat vain valtuutettujen henkilöiden saatavilla.
- Eheys tarkoittaa sitä, että tiedot säilytetään täydellisinä ja tarkkoina.
- Saatavuus tarkoittaa sitä, että valtuutetut henkilöt saavat tarpeen mukaan tietoja käyttöönsä.

Näiden tavoitteiden saavuttamiseksi organisaatiossa on tehtävä riskienarviointi, jossa selvitetään tietovaroihin kohdistuvia mahdollisia riskejä. Tämän jälkeen voidaan rakentaa tietoturvan hallintajärjestelmä, jolla riskejä on mahdollista hallita tehokkaasti ilman tarpeettomia kustannuksia tai tuottavuuden menetystä.

Riskienarviointi Atealla

Seuraavat Atean liiketoimintaa uhkaavat tietoturvariskit on määritetty ensisijaisiksi:

1. **Laitteiston katoaminen ja tilaturvallisuus:** Tietovaroja tallennetaan laitteisiin, jotka on mahdollista kadottaa, varastaa tai ne voivat vahingoittua. Kulunvalvonta, salaus ja tietojen varmuuskopiointi ovat esimerkkejä riskien rajoittamiseksi. Tätä tehdään tietokoneisiin, matkapuhelimiin, palvelimiin ja tallennuslaitteisiin. Konesalit ovat erityisen haavoittuvia, ja niitä on suojattava ympäristön aiheuttamilta vaaroilta, kuten ennakoimattomilta lämpötiloilta ja tulipalolta.

2. **Identiteettipetos**
   Atea on jatkuvasti petosyritysten kohteena, joissa hyökkääjät käyttävät vääriä identiteettejä tai petosta voittaakseen työntekijän luottamuksen. Petosyrityksen tavoitteena on varastaa Atean omaisuutta tai saada luvaton pääsy Atean järjestelmiin ja verkkoihin.

   Eräs identiteettipetosten tyyppi on käyttää väärennettyjä tai varastettuja asiakastietoja IT-laitteiden tilaamiseen, erityisesti Atean verkkokaupassa. Verkkokaupan pääsynvalvonnan lisäksi Atealla on liiketoimintarutiineja uusien asiakastilien seulomiseen ja epätavallisen asiakastoiminnan tunnistamiseen olemassa olevilla tileillä. Näin voidaan vähentää vilpillisten asiakkuuksien riskiä.

   Tietojen kalastelu on yksi tavallisimmista huijaustyypeistä. Siinä rikollinen ottaa yhteyttä suoraan Atean työntekijään, useimmiten sähköpostitse. Sähköposti näyttää olevan peräisin luotettavasta lähteestä ja lähettäjä hyödyntää usein väärennettyä identiteettiä. Hän voi esiintyä esimerkiksi Atean toisena työntekijänä, liikekumppanina tai teknologiayrityksen tai pankin edustajana. Sähköpostin on tarkoitus huijata Atean työntekijää esimerkiksi siirtämään rahaa, paljastamaan käyttäjätunnus, salasana tai muita arkaluontoisia tietoja tai napsauttamaan linkkiä tai liitetiedostoa, jolloin tietokoneelle tai mobiililaitteelle ladataan haittaohjelma.

   Sähköpostiviesti, liite tai linkki näyttää viattomalta. Se on esimerkiksi naamioitu kollegan viestiksi, toimittajan tarjoukseksi/laskuksi tai ilmoitukseksi,vaikkapaOneDrivesta.Tästäsyystä Atean työntekijöiden on oltava varuillaan sähköposteihin ja muuhun viestintään liittyvien petosten suhteen, vaikka viesti vaikuttaisi tulevan luotetusta lähteestä.

   Atean työntekijät eivät saa avata linkkejä tai liitetiedostoja omilta laitteiltaan, jos heillä on epäilyksiä sähköpostin tai viestin alkuperästä. Jos Atean työntekijä on epävarma sähköpostin turvallisuudesta tai jos hän on vahingossa vastannut mahdolliseen petosyritykseen avaamalla epäilyttävän linkin tai liitetiedoston, hänen tulee ottaa välittömästi yhteyttä Atean palvelupisteeseen.

Vaikka sähköpostiviestintä on työpaikoilla tavallisin tietojenkalastelussa käytetty menetelmä, Atean työntekijöiden tulee varoa myös muuta petollista viestintää, kuten puhelinsoittoja ja sosiaalisen median kutsuja.

3. Liikesalaisuuksien varastaminen:

Jos luvattomilla henkilöillä on pääsy Atean tietojärjestelmiin, he saattavat yrittää varastaa luottamuksellisia, Atean liiketoiminnan kannalta arkaluontoisia tietoja. Niihin voi kuulua salaisia yritystietoja, kuten asiakkaan tai toimittajan tietoja, sopimuksia ja kaupallisia ehtoja. Tietoihin voi sisältyä myös immateriaaliomaisuutta, kuten liiketoiminta-konsepteja, tuotetai palvelumalleja sekä sisäisesti kehitettyjä ohjelmistoja, menetelmiä ja työkaluja.

Työntekijät, joilla on pääsy tärkeimpiin järjestelmiin, voivat myös yrittää varastaa Atean liikesalaisuuksia, erityisesti jos he aikovat lähteä yrityksestä. Järjestelmän käyttöoikeuksia olisi jatkuvasti valvottava sen varmistamiseksi, että tiedot ovat vain niitä tarvitsevien saatavilla ja että käyttäjän käyttöoikeudet suljetaan, kun niitä ei enää tarvita.

Pääsynvalvonnan lisäksi Atea käyttää SIEM-työkaluja (Security Information and Event Management) lokitietojen ja järjestelmien käytön analysoimiseen.

4. Liiketoiminnan häiriöt:

Atean liiketoiminta on riippuvaista IT-järjestelmistä. Jos pääsynvalvontaa rikotaan tai järjestelmiä käytetään väärin, työntekijöiden tai liikekumppanien yksityiset tiedot voivat päästä vuotamaan. Atean liiketoiminnan kannalta tarpeellista tietoa voidaan peukaloida tai poistaa. Luvattomat henkilöt voivat myös tehdä tai hyväksyä liiketoimia Atean hallinnon valvontatoimien vastaisesti. Kaikki nämä tapahtumat häiritsevät Atean liiketoimia.

On myös olemassa vaara, että Atean toimintaa häiritään taidokkaalla hakkerointihyökkäyksellä, joka sulkee keskeiset tietojärjestelmät tai -verkot. Järjestelmät saattavat saada tartunnan haittaohjelmista, jotka estävät käyttäjiä pääsemästä kriittisiin toimintoihin tai lukemaan datatiedostoja, elleivät he maksa lunnaita (”ransomware”). Verkkoon tai palvelimiin saatetaan tehdä valtava määrä käyntejä tai pyyntöjä, jolloin ne eivät enää pysty käsittelemään normaaleja liiketoimia (“palvelunestonestohyökkäys”). Nämä hyökkäykset voivat kohdistua joko Ateaan tai asiakkaisiin, joita Atea hallinnoi tietokeskuksestaan.

5. Sopimussuhteiden vahingot:

Atealla on salassapitosopimuksia useiden asiakkaiden, toimittajien ja liikekumppanien kanssa. Lisäksi Atealla on palvelutasosopimuksia ja tietojenkäsittelysopimuksia asiakkaiden kanssa, jotka hankkivat Atealta tietotekniikkapalveluja ja tukea.

Tietoturvapoikkeama Atealla voi johtaa luottamuksellisuuden, palvelutason ja tietojenkäsittelysopimuksen rikkomukseen. Se voi johtaa Ateaa vastaan nostettuun kanteeseen, jossa Ateaa vaaditaan korvaamaan sopimusrikkeistä aiheutuneet vahingot. Suorien vahinkojen lisäksi tietoturvapoikkeama voi aiheuttaa pitkäkestoista vahinkoa Atean liikesuhteille asiakkaiden ja kumppaneiden kanssa.

Jopa sellaisissa tilanteissa, joissa sopimusta ei ole solmittu, Atea voi joutua vastaamaan yrityksien tai yksityishenkilöiden oikeudellisiin vaatimuksiin, jos heidän tietojaan varastetaan tai käytetään väärin, eikä Atea ole osoittanut asianmukaista huolellisuutta niiden käsittelyssä.

6. Sääntömääräiset seuraamukset:

Oslon pörssiin listattuna yrityksenä Atean on noudatettava tiukkoja lakisääteisiä vaatimuksia käsitellessään tietoja, jotka eivät ole markkinoiden tiedossa ja joilla voi olla vaikutus Atean osakkeen arvoon (hintaan vaikuttavat tiedot). Niihin voi sisältyä tietoja merkittävistä uusista sopimuksista tai taloudellisista tuloksista, joista ei ole vielä kerrottu julkisesti.

Atean on hallinnoitava hintaan vaikuttavia tietoja luottamuksellisesti, jotta niitä ei jaeta muille kuin rajoitetulle määrälle sellaisia sisäpiiriin kuuluvia henkilöitä, joiden tarvitsee ne tietää. Tällaisia hintaan vaikuttavia tietoja hallussaan pitävät työntekijät on rekisteröitävä. Heitä koskevat juridiset erityisvaatimukset, jotka liittyvät salassapitoon ja Atean osakkeiden kaupankäyntirajoituksiin. Näiden juridisten vaatimusten rikkominen voi johtaa syytteeseen ja lakisääteisiin seuraamuksiin Norjan arvopaperikauppalain mukaisesti.

Euroopan unionin yleisen tietosuoja-asetuksen (GDPR) nojalla Atealle on mahdollista määrätä seuraamuksia tietosuoja-asetuksen rikkomisesta. Koska GDPR:n vaatimukset ovat laajoja, aihe käsitellään erikseen tämän asiakirjan seuraavassa tietosuojaa käsittelevässä osassa.

Kertaus:

Kaikkien työntekijöiden on oltava erittäin varovaisia tietojen ja IT-järjestelmien käsittelyssä tietoturvarikkomusten ehkäisemiseksi.

IT-laitteita voidaan kadottaa, varastaa tai vahingoittaa. Kulunvalvonta, salaus ja tietojen varmuuskopiointi ovat siksi välttämättömiä mahdollisten tietoturvariskien rajoittamiseksi.

Atea altistuu jatkuvasti petosyrityksille, joissa hyökkääjät käyttävät vääriä identiteettejä tai petosta voittaakseen työntekijän luottamuksen. On huomioitava, että mikä tahansa vastaanottamasi sähköpostiviesti tai muu yhteydenotto voi olla petosyritys, vaikka se näyttäisi olevan peräisin asiallisesta lähteestä (mukaan lukien sähköpostiviestit Atean johtajalta, asiakkaalta, teknologiatoimittajalta tai sosiaalisen median tililtä).

Ole varuillasi, mikäli havaitset epätavallista viestintää tai toimintaa. Jos epäilet, että olet joutunut petosyrityksen kohteeksi sähköpostitse tai muulla viestillä, ota yhteyttä Atean palvelupisteeseen. Älä vastaa epäilyttävään viestiin. Älä esimerkiksi avaa sähköpostiliitteitä ja ulkoisia linkkejä tai käsittele tilauksia ja maksuja.

Tietojen varkauden tai väärinkäytön riskin vähentämiseksi työntekijöille on annettava tiedonsaantioikeus vain tarpeen perusteella. Järjestelmän käyttöoikeuksia tulisi jatkuvasti tarkistaa sen varmistamiseksi, että käyttöoikeudet lopetetaan, kun niitä ei enää tarvita.

Tietoturvapoikkeama voi aiheuttaa vakavaa vahinkoa Atealle. Se voi johtaa liiketoiminnan keskeytymiseen, Atean sopimusvelvoitteiden rikkomuksiin, lakisääteisiin seuraamuksiin sekä Atean maineen ja liikesuhteiden vahingoittumiseen.

2. TIETOSUOJA – YLEISKUVA JA RISKIENHALLINTA

Tietosuojaan kuuluu se, että henkilö hallitsee omia tietojaan - erityisesti mahdollisuus määrittää, milloin ja miten tietoja kerätään, jaetaan ja käytetään. Henkilötiedot määritellään tiedoiksi, jotka voidaan yhdistää tiettyyn ja tunnistettavaan henkilöön.

Tietosuoja on riippuvainen tietoturvasta eli siitä, miten tiedot suojataan luvattomalta käytöltä ja väärinkäytöltä. Tietosuoja on kuitenkin tietoturvaa laajempi käsite, sillä se kattaa myös yksilön tietoja koskevien oikeuksien suojaamisen. Erityisesti kyse on siitä, miten jokainen voi hallita organisaation keräämien ja käsittelemien henkilötietojensa käyttöä.

Me Atealla uskomme, että tietosuoja on perustavanlaatuinen ihmisoikeus. Olemme sitoutuneet käsittelemään henkilötietoja tätä oikeutta kunnioittaen. Atean on käsiteltävä henkilötietoja Euroopan unionin yleisen tietosuojaasetuksen (GDPR) tiukkojen vaatimusten mukaisesti.

GDPR-vaatimukset Atealla voidaan tiivistää seuraavasti:

Henkilötietojen keräämistä koskevat vaatimukset
Atea voi käsitellä (esimerkiksi kerätä, tallentaa ja käyttää) henkilötietoja vain, jos siihen on oikeutettu liiketoiminnallinen peruste tai, jos asianomainen henkilö on antanut suostumuksensa, tai hän on saanut ilmoituksen henkilötietojensa käsittelystä. Ilmoitusta ja suostumusta koskevat yksityiskohdat on kuvattu tämän asiakirjan seuraavassa osassa.

Yksilön oikeus hallita henkilötietojaan
Atean on noudatettava yksilön henkilötietojen käyttöä koskevaa pyyntöä GDPR:ssä yksilölle määritettyjen oikeuksien mukaisesti. GDPR:n mukaisesti, jokaisella on tiedonsaantioikeus Atean käsittelemiin henkilötietoihinsa. Henkilöillä on oikeus korjata henkilötiedoissaan olevia virheitä, pyytää henkilötietojensa poistamista tai rajoittaa tietojensa käsittelyä ja käyttöä.

Käsittelytoimien dokumentointi
Atean on dokumentoitava henkilötietojen käsittelyn laajuus. Tähän pitää sisältyä kuvaus rekisteröityjen ryhmistä sekä siitä, millaisia henkilötietoja käsitellään. Lisäksi tulee kuvata, mitä teknisiä ja organisatorisia toimenpiteitä on toteutettu tietosuojarikkomuksen vaikutusten ehkäisemiseksi ja minimoimiseksi (”privacy by design”).

Tietojenkäsittelysopimukset (DPA) asiakkaiden/toimittajien kanssa
Kun Atea tarjoaa asiakkailleen tietojenkäsittelypalveluita (esimerkiksi hallinnoi asiakkaiden tietoinfrastruktuuria ja sovelluksia joko asiakkaan tiloissa tai omassa konesalissaan), Atealla on oltava asiakkaan kanssa voimassa oleva tietojenkäsittelysopimus, joka täyttää GDPR-vaatimukset.

Vastaavasti silloin, kun Atea käsittelee henkilötietoja alihankkijan tai toimittajan kautta (esimerkiksi käyttäessään toimittajan konesalissa operoitavia ohjelmistosovelluksia, kuten pilvipalveluja), Atealla on oltava voimassa oleva GDPR-yhteensopiva tietojenkäsittelysopimus ko. tahon kanssa. EU:n/ETA-alueen ulkopuolella käsiteltävän tiedon on sijaittava sellaisessa maassa, jonka viranomaiset ovat hyväksyneet riittävät tietosuojatoimenpiteet toteuttavana maana.

Henkilötietojen tietoturvaloukkaukseen liittyvät vaatimukset
Jos henkilötietoihin kohdistuva loukkaus voi aiheuttaa haittaa yksilölle, Atean on ilmoitettava asiasta sen maan valvontaviranomaiselle, jossa rikkomus tapahtui, 72 tunnin kuluessa siitä, kun se on tullut tietoiseksi asiasta. Ilmoituksessa kerrotaan tietoturvaloukkauksen tyyppi, lista asianomaisista rekisteröidyistä ja loukkauksen kohteena olevista henkilötietojen tyypeistä sekä tietoturvaloukkauksen todennäköiset seuraukset ja toimenpiteet, joihin on ryhdytty.

Henkilöille, joiden henkilötietoja loukkaus koskee, on myös ilmoitettava asiasta suoraan, mikäli loukkauksesta voi aiheutua suuri vahingon riski kyseiselle henkilölle. Julkinen viestintä voi riittää, jos henkilökohtaista ilmoitusta ei ole mahdollista tehdä.

GDPR-asetuksen mukaisesti jokaisen maan valvontaviranomainen voi määrätä yrityksselle korkeat seuraamusmaksut GDPR-rikkomuksesta. Seuraamuksen määrä perustuu rikkomuksen luonteeseen, vahingon laajuuteen ja toimenpiteisiin, joita yritys on toteuttanut rikkomuksen estämiseksi ja korjaamiseksi. GDPR:ään perustuvan sanktion enimmäismäärä on 4 % yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta tai 20 miljoonaa euroa, riippuen siitä, kumpi näistä on suurempi.

GDPR-vaatimusten vuoksi on olennaista, että Atea dokumentoi kaikki sellaiset toimenpiteet, joiden puitteissa käsitellään henkilötietoja, sekä tunnistaa kaikki sisäiset sovellukset ja sopimukset, joihin liittyy henkilötietoja. Näiden tietojen on oltava kunkin maan tietoturvajohtajan saatavilla asianmukaisen tietosuojatason varmistamiseksi. Kunkin maan ja konsernin tietoturvajohtajat löytyvät Atean Compliance-sivustolta.

Kertaus:

Tietosuojaan kuuluu se, että henkilö hallitsee omia tietojaan - erityisesti mahdollisuus määrittää, milloin ja miten tietoja kerätään, jaetaan ja käytetään. Henkilötiedot määritellään tiedoiksi, jotka voidaan yhdistää tiettyyn ja tunnistettavaan henkilöön.

Atean on käsiteltävä henkilötietoja Euroopan unionin yleisen tietosuojaasetuksen (GDPR) tiukkojen vaatimusten mukaisesti.

GDPR-asetuksen mukaisesti:

Atea voi käsitellä (esimerkiksi kerätä, tallentaa ja käyttää) henkilötietoja vain, jos siihen on oikeutettu liiketoiminnallinen peruste tai, jos asianomainen henkilö on antanut suostumuksensa, tai saanut ilmoituksen henkilötietojensa käsittelystä.

Atean on noudatettava yksilön henkilötietojen käsittelyyn liittyvää pyyntöä GDPR:ssä yksilölle määritettyjen oikeuksien mukaisesti.

Atean on dokumentoitava käsittelytoimenpiteidensä laajuus, mukaan lukien toimenpiteet, joita on toteutettu tietosuojarikkomuksen vaikutuksen estämiseksi ja minimoimiseksi. Tämä edellyttää sitä, että Atea dokumentoi kaikki sellaiset toimenpiteet, joiden puitteissa käsitellään henkilötietoja, sekä tunnistaa kaikki sisäiset sovellukset ja sopimukset, joihin liittyy henkilötietoja.

Atealla on oltava voimassa oleva tietojenkäsittelysopimus kaikkien niiden asiakkaiden kanssa, joille se tarjoaa tietojenkäsittelypalveluita (esimerkiksi tietoinfrastruktuurin ja sovellusten hallinta asiakkaan tiloissa tai Atean konesalissa).

Atealla on myös oltava voimassa oleva tietojenkäsittelysopimus sellaisen alihankkijan tai toimittajan kanssa, joka käsittelee henkilötietoja Atean puolesta tai sen lukuun (esimerkiksi tarjoamalla ohjelmistosovelluksia, joita operoidaan toimittajan konesalissa, kuten pilvipalvelut).

Jos henkilötietoihin kohdistuva tietoturvaloukkaus voi aiheuttaa haittaa yksilölle, Atean on ilmoitettava asiasta sen maan valvontaviranomaiselle, jossa rikkomus tapahtui, 72 tunnin kuluessa siitä, kun se on tullut tietoiseksi asiasta.

3. TIETOSUOJAKÄYTÄNNÖT ATEALLA

Atean työntekijöiden on noudatettava yrityksen tietosuojakäytäntöjä aina kerätessään, käsitellessään ja jakaessaan henkilötietoja. Kaikki Atean esimiehet vastaavat siitä, että heidän vastuullaan olevissa liiketoimintaprosesseissa noudatetaan Atean tietosuojakäytäntöjä ja että heidän työntekijänsä toimivat näiden liiketoimintaprosessien mukaisesti.

Kaikille Atean esimiehille on määritetty tietosuojaylläpitäjä (Data Protection Administrator), joka vastaa tietystä toiminteesta omassa maassaan. Tietosuojaylläpitäjän tehtävänä on varmistaa, että kaikissa hänen toiminteensa liiketoimintaprosesseissa noudatetaan Atean tietosuojakäytäntöjä. Esimerkkejä toiminteista: myynti/markkinointi, HR, talous, konsultointi, AMS, logistiikka ja IT.

Jokaisen toiminteen tietosuojaylläpitäjä raportoi oman maansatietoturvajohtajalle (Chief Information Security Officer). Jokaisen maan tietoturvajohtajalla on yleinen vastuu tietosuojakäytäntöjen toteuttamisesta kyseisessä maassa. Hän raportoi konsernin tietoturvajohtajalle.

Löydät oman maasi tietoturvaorganisaation keskeisten jäsenten nimet Atean Compliance-sivustosta: atea.com/trust. Tietosuojaorganisaation yhteenveto on myös tämän asiakirjan liitteessä.

Atean tietosuojaan liittyvät toimintaperiaatteet kattavat seuraavat aiheet:

- Järjestelmien rekisteröinti
- Tietojen luokittelu
- Henkilötietojen hallinta
- Asiakassopimukset

Yhteenveto tietosuojaan liittyvistä toimintaperiaatteista:

Järjestelmien rekisteröinti

Ennen kuin Atean työntekijä aloittaa prosessin henkilötietojen keräämiseksi, käsittelemiseksi tai jakamiseksi, hänen on varmistettava, että kaikki tietoja tallentavat tai käsittelevät järjestelmät on rekisteröity ja hyväksytty maan tietoturvajohtajan toimesta. Tähän lukeutuvat pilvipalvelut, jotka hankitaan tilausperusteisesti ja, joita hallitaan Atean ulkopuolella.

Tietoturvajohtaja analysoi järjestelmän tietoturva- ja tietosuojastandardit ennen kuin se hyväksytään ja rekisteröidään käyttöön Atealla. Analyysi perustuu Atean tietoturva- ja tietosuojastandardien tarkistuslistaan, ja se täytetään yhdessä Atea-konsernin tietoturvajohtajan kanssa.

Tietoturvajohtaja huomioi myös järjestelmään tallennettavien tietojen tyypin ja arkaluontoisuuden, kun hän analysoi sitä, täyttääkö järjestelmä Atean tietoturvavaatimukset. Osana analyysia tietoturvajohtaja kuvaa myös käytännön henkilötietojen poistamiseksi järjestelmästä, kun Atea ei enää tarvitse niitä (tietojen minimointikäytäntö).

Jos järjestelmää hallinnoidaan ulkoisesti ja se sisältää henkilötietoja – esimerkiksi pilvipohjainen HR-järjestelmä –, Atealla on oltava allekirjoitettu tietojenkäsittelysopimus (DPA) palveluntarjoajan kanssa GDPR:n noudattamiseksi. Pilvipalveluntarjoajan kanssa käytettävä vakiomuotoinen DPA-sopimus on saatavilla kunkin maan intranetin Global Information Security-sivulta. Kunkin maan tietoturvajohtaja vastaa DPA-sopimusta koskeviin kysymyksiin ja tarjoaa tukea allekirjoitetun sopimuksen saamiseksi.

Atean työntekijät eivät saa tallentaa tai käsitellä yrityksen tietoja niin kutsutuissa shadow-IT-järjestelmissä, joita heidän maansa tietoturvajohtaja ei ole rekisteröinyt. Atean työntekijät eivät saa tehdä merkittäviä muutoksia tietojenkäsittelyjärjestelmiin tai -prosesseihin ilmoittamatta niistä tietoturvajohtajalle.

Kun järjestelmä on hyväksytty käytettäväksi Atealla, sille määritetään omistaja. Järjestelmän omistaja vastaa siitä, että järjestelmää käytetään Atean tietosuojakäytäntöjen mukaisesti. Omistaja on erityisesti vastuussa siitä, että käyttöoikeudet tietojärjestelmään rajoittuvat vain niille henkilöille, jotka tarvitsevat pääsyn järjestelmään. Käyttöoikeudet on myös lopetettava heti, kun niitä ei enää tarvita. Järjestelmän omistajan on myös varmistettava, että järjestelmään tallennetut henkilötiedot poistetaan, kun Atea ei enää tarvitse niitä. Näin noudatetaan tietojen järjestelmän käyttöönottovaiheessa määriteltyä minimointikäytäntöä.

Tietojen luokittelu

Kun järjestelmä hyväksytään käytettäväksi Atealla, siihen tallennettujen tietojen tyyppi ja arkaluontoisuus dokumentoidaan. Näin voidaan varmistaa, että asianmukaisia tietosuojakäytäntöjä ylläpidetään.

Monissa tilanteissa Atean työntekijät joutuvat käsittelemään ja jakamaan tietoa hyväksytyn IT-järjestelmän ulkopuolella. Kyseessä voivat olla esimerkiksi painetut asiakirjat, sähköpostiviestintä tai tiedoston jakaminen (Microsoft Word / Excel / Powerpoint).

Jotta voidaan varmistaa, että hyväksytyn IT-järjestelmän ulkopuolella käsiteltäviä tietoja hallinnoidaan asianmukaisella tietoturvatasolla, Atean työntekijöiden on merkittävä kaikki tiedostot, asiakirjat tai sähköpostiviestit niiden arkaluontoisuuden mukaan. Merkintä on tehtävä Atean tietojen luokittelustandardien mukaisesti.

Atean tietojen luokittelustandardit koostuvat viidestä tasosta, jotka luokittelevat sähköpostin tai tiedoston niiden arkaluontoisuuden mukaan. Luokittelustandardit on sisäänrakennettu Atean versioihin Microsoft Outlookista ja Word/Excel/Powerpoint-ohjelmista. Atean työntekijät voivat automaattisesti merkitä sähköpostiviestin, asiakirjan tai tiedoston asianmukaisella luokittelustandardilla valitsemalla painikkeen ohjelmistojen otsikkoriviltä.

Luokittelustandardien viisi tasoa:

1. Non-Business:
Yksityiset sähköpostiviestit ja asiakirjat, jotka eivät liity Ateaan.

2. Public: Ateaan liittyvät tiedot, joita voidaan jakaa julkisesti.

3. Internal: Tiedot, joita voidaan jakaa vapaasti Atean sisällä tai sopimustoimittajien ja alihankkijoiden kanssa. Tietoja ei ole tarkoitettu jaettavaksi ulkopuolisille.

4. Confidential:
Tiedot, jotka on pidettävä vain vastaanottajan tietona, ja joita ei saa jakaa ilman tietojen omistajan hyväksyntää. Näihin kuuluvat henkilötiedot, jotka tulee merkitä erikseen. Henkilötietojen merkintä voidaan tehdä Confidential-painikkeella avattavasta valikosta.

5. Strictly confidential:
Tiedot, joilla olisi merkittäviä haitallisia vaikutuksia Atealle, mikäli niitä paljastettaisiin luvattomasti. Nämä tiedot on säilytettävä salatussa muodossa,eikäniitäsaajakaailmantietojenomistajan hyväksyntää. Mukaan lukien:

- Arkaluontoiset henkilötiedot: GDPR-asetuksen mukaan tiettyihin kategorioihin kuuluvien henkilötietojen käsittelyssä on noudattava erityistä varovaisuutta. Näihin kuuluvat tiedot, jotka liittyvät etniseen alkuperään, poliittisiin mielipiteisiin, uskontoon, ammattiyhdistysten jäsenyyteen sekä geneettisiin tai biometrisiin tietoihin. Arkaluontoiset henkilötiedot tulee merkitä erikseen. Merkintä voidaan tehdä Strictly confidential -painikkeella avattavasta valikosta.

- Arkaluontoiset liiketoimintatiedot: Salaiset yritystiedot, kuten avainasiakkaan tai toimittajan tiedot, sopimukset ja kaupalliset ehdot. Niiksi luetellaan myös tiedot, joista on tehty salassapitosopimus asiakkaan tai liikekumppanin kanssa. Lisäksi, myös erittäin arkaluontoiset immateriaalioikeudet, kuten liiketoimintakonseptit, tuote- tai palvelumallit sekä sisäisesti kehitetyt ohjelmistot, menetelmät ja työkalut voidaan luokitella arkaluontoisiksi liiketoimintatiedoiksi.

- Hintaan vaikuttavat tiedot: Hintaan vaikuttavat tiedot ovat erityinen luottamuksellisten tietojen tyyppi, joka voi vaikuttaa Atean osakkeen hintaan. Tähän sisältyvät merkittävät taloudelliset tiedot, joista ei ole vielä raportoitu, tai erittäin laajat asiakassopimukset tai kaupalliset sopimukset, jotka liittyvät luottamuksellisiin neuvotteluihin.

- Atea-konsernin talousjohtajalle on kerrottava välittömästi kaikista työntekijöistä, joilla on hintaan vaikuttavia tietoja. Nämä työntekijät rekisteröidään Atean käyttämään Computershare Insider Management System (CIMS) -järjestelmään. Lisätietoa hintaan vaikuttaviin tietoihin liittyvistä menettelyistä löytyy Atean eettisistä ohjeista.

Laajempi kuvaus Atean tietojen luokitusstandardeista ja asiakirjojen merkitsemis- ja salausmenetelmistä sekä sähköpostiviestinnästä löytyy oman maasi intranetin Global Information Security -sivustosta.

Henkilötietojen hallinta

GDPR-asetuksen mukaisesti Atealla on erityisiä oikeudellisia velvoitteita henkilötietojen, eli tiettyyn ja tunnistettavaan henkilöön yhdistettävien tietojen, käsittelyssä. Näiden oikeudellisten velvoitteiden mukaisesti Atean on dokumentoitava, että se on ryhtynyt riittäviin teknisiin ja organisatorisiin toimenpiteisiin GDPR:n noudattamiseksi. Prosessidokumentaation on oltava pyynnöstä viranomaisen saatavilla.

Ennen kuin Atea voi kerätä henkilötietoja, liiketoimintaprosessi, jonka puitteissa henkilötietoja käsitellään, on dokumentoitava kattavasti ja tietoturvajohtajan on tarkastettava se. Kunkin toiminteen tietosuojaylläpitäjä vastaa siitä, että kaikki toiminteen henkilötietojen käsittelyprosessit on dokumentoitu ja ajan tasalla GDPR:n mukaisesti.

Asiakirjoista on käytävä ilmi, että Atea on ryhtynyt riittäviin teknisiin ja organisatorisiin toimenpiteisiin, jotta se voi kunnioittaa yksilön oikeuksia henkilötietoihinsa, estää ja minimoida henkilötietojen tietoturvarikkomusten vaikutukset ja reagoida niihin lainsäädännön vaatimalla tavalla. Prosessidokumentaation on sisällyttävä myös tietojen minimointi, eli tietojen poistaminen, kun Atea ei enää tarvitse niitä.

Henkilötietoja kerätessään Atean on ilmoitettava asiasta kyseiselle henkilölle tai pyydettävä hyväksyntä tietojen keräämiseen ja käyttöön. Kun henkilölle ilmoitetaan henkilötietojen käytöstä tai siihen pyydetään lupaa, Atean on annettava seuraavat tiedot GDPR:n mukaisesti:

1. Kerättävien ja käsiteltävien henkilötietojen tyypit
2. Käsittelyn tarkoitus ja oikeusperusta
3. Henkilötietojen vastaanottajat tai vastaanottajaryhmät
4. Aika, jona tietoja käytetään, tai perusteet, jotka määrittelevät tämän ajanjakson
5. Yksilön oikeudet omiin henkilötietoihinsa – mukaan lukien oikeus peruuttaa suostumus ja oikeus saada tiedot poistetuksi tai korjatuksi
6. Yksilön oikeus valittaa valvontaviranomaiselle
7. Tarvittaessa ilmoitus siitä, että tiedot siirretään toiseen maahan, ja vahvistus siitä, että tietojen käsittely toisessa maassa on GDPR-asetuksen tietosuojan riittävyyttä koskevien säännösten mukainen.
8. Arkaluontoisia henkilötietoja kerätessään Atean on pyydettävä ja saatava yksiselitteinen suostumus siltä henkilöltä, jonka tiedoista on kyse.

Henkilötietojen keräämistä koskeva tietosuojaseloste on saatavilla kunkin maan intranetin Global Information Security -sivulta.

Atealla on GDPR:n mukaan erityisiä velvoitteita tietoturvarikkomuksiin liittyen. Tietoturvaloukkaus tarkoittaa tilannetta, jossa luvattomat henkilöt pääsevät käsiksi tietoihin tai aiheuttavat tietojen laittoman tai tahattoman menetyksen.

Tietoturvaloukkauksen tapahtuessa Atean työntekijöiden on välittömästi ilmoitettava asiasta oman maansa tietoturvajohtajalle. Tietoturvajohtaja tutkii tietoturvaloukkausta yhdessä Atean tietoturvaorganisaation kanssa ja ryhtyy tarvittaessa korjaaviin toimiin rikkomuksesta aiheutuvien vahinkojen raportoimiseksi ja lieventämiseksi.

Jos tietoturvaloukkaus koskee henkilötietoja ja se voi aiheuttaa haittaa yksilölle, Atean on ilmoitettava asiasta sen maan valvontaviranomaiselle, jossa rikkomus tapahtui, 72 tunnin kuluessa siitä, kun se on tullut tietoiseksi asiasta. Ilmoituksessa kerrotaan tietoturvaloukkauksen tyyppi, lista asianomaisista rekisteröidyistä ja henkilötietoja sisältävistä rekistereistä, tietoturvaloukkauksen todennäköiset seuraukset ja toimenpiteet, joihin on ryhdytty.

Henkilöille, joiden henkilötietoja tietoturvaloukkaus koskee, on myös ilmoitettava asiasta suoraan, mikäli rikkomuksesta voi aiheutua suuri vahingon riski kyseiselle henkilölle. Julkinen viestintä voi riittää, jos henkilökohtaista ilmoitusta ei ole mahdollista tehdä.

Asiakassopimukset

Atea hallinnoi monien asiakkaiden tietoinfrastruktuuria ja sovelluksia joko asiakkaan tiloissa tai oman datakeskuksensa kautta. Näissä tapauksissa Atea vastaa sopimusperusteisesti asiakkaan tietojen käsittelystä, ja Atealla on GDPR:n mukaan lakisääteinen velvollisuus varmistaa, että se suojaa riittävästi niiden henkilöiden tietosuojaa koskevia oikeuksia, joiden henkilötietoja se käsittelee asiakassopimuksen perusteella.

GDPR-vaatimusten täyttämiseksi Atealla on oltava asiakkaidensa kanssa

tietojenkäsittelysopimus (DPA), kun se hallinnoi asiakkaan tietoinfrastruktuuria ja sovelluksia. Tietojenkäsittelysopimuksessa on dokumentoitava asiakkaan ohjeisiin perustuvien käsittelytoimenpiteiden laajuus, luonne ja kesto. Dokumentaatiossa tulee olla myös yhteenveto siitä, millaisia henkilötietoja Atea käsittelee asiakkaan puolesta ja millaisten henkilöryhmien tietoja käsitellään.

Tietojenkäsittelysopimuksen tulee sisältää seuraavat tiedot GDPR-asetuksen mukaisesti:

1. Atea käsittelee henkilötietoja vain asiakkaan dokumentoitujen ohjeiden mukaisesti ja noudattaa tietosuojalainsäädäntöä.
2. Atean työntekijät, jotka käsittelevät henkilötietoja asiakkaan puolesta, ovat sitoutuneet luottamuksellisuuteen. Atea ei käytä alihankkijoita asiakkaan henkilötietojen käsittelyyn ilman asiakkaan lupaa.
3. Atea on ryhtynyt riittäviin teknisiin ja organisatorisiin toimenpiteisiin varmistaakseen asiakkaan kanssa sovitun turvallisuustason käsiteltäviin tietoihin liittyvien riskien mukaan.
4. Atea on ryhtynyt riittäviin toimenpiteisiin niiden oikeudellisten velvoitteiden täyttämiseksi, jotka koskevat henkilöiden oikeutta valvoa tietojensa käsittelyä, kuten GDPR-asetuksessa on kuvattu.
5. Atea toimittaa asiakkaalle kaikki tarvittavat tiedot sen osoittamiseksi, että se noudattaa GDPR:n mukaisia tietosuojavelvoitteita ja osallistuu pyydettäessä asiakkaan vaatimustenmukaisuustarkastukseen.
6. Atea ilmoittaa asiakkaalle henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä.
7. Atea poistaa tai palauttaa kaikki henkilötiedot asiakkaalle palvelusopimuksen päättyessä.

Jos Atea käyttää alihankkijoita täyttääkseen tietojenkäsittelyvelvoitteensa (esimerkiksi kolmannen osapuolen pilvipalveluita, konsultteja tai infrastruktuurin tarjoajia), näiden alihankkijoiden kanssa on solmittava erillinen tietojenkäsittelysopimus, jossa alihankkija sitoutuu edellä kuvattua asiakassopimusta vastaaviin velvoitteisiin.

Atealla on vakiomuotoinen tietojenkäsittelysopimus, jota suositellaan käytettäväksi kaikkien asiakkaiden ja alihankkijoiden kanssa. Tietojenkäsittelysopimus on saatavilla kunkin maan intranetin Global Information Security-sivulta. Kunkin maan tietoturvajohtaja vastaa DPA-sopimusta koskeviin kysymyksiin ja tarjoaa tukea allekirjoitetun sopimuksen saamiseksi.

Jos henkilötietojen tietoturvaloukkaus koskee asiakkaan tietoja, Atean on ilmoitettava asiakkaalle heti, kun se tulee tietoiseksi asiasta. Atean on tehtävä yhteistyötä asiakkaansa kanssa ja toteutettava kohtuulliset toimenpiteet sen varmistamiseksi, että asiakas voi täyttää GDPR-asetuksen määrittämät velvollisuutensa raportoida tietoturvarikkomuksesta ja toteuttaa korjaavat toimenpiteet rikkomuksen aiheuttamien vahinkojen lieventämiseksi.

Kertaus:

Järjestelmien rekisteröinti

Kaikki Atealla käytettävät IT-järjestelmät on rekisteröitävä tietoturvajohtajalla (Chief Information Security Officer) siinä maassa tai liiketoimintayksikössä, jossa järjestelmää käytetään. Tähän lukeutuvat pilvipalvelut, jotka hankitaan tilausperusteisesti ja joita hallitaan Atean ulkopuolella.

Tietoturvajohtaja tarkastaa IT-järjestelmän sen vahvistamiseksi, että se täyttää Atean IT-turvallisuusstandardit ennen järjestelmän hyväksymistä käyttöön. Kun järjestelmä on rekisteröity, sille määritetään omistaja. Järjestelmän omistajan tehtävänä on vastata siitä, että järjestelmää käytetään Atean tietosuojakäytäntöjen mukaisesti ja erityistä huomiota kiinnitetään käyttöoikeuksien hallintaan.

Tiedon luokittelu

Jotta voidaan varmistaa, että rekisteröidyn IT-järjestelmän ulkopuolella tietoja hallinnoidaan asianmukaisella tietoturvatasolla, Atean työntekijöiden on merkittävä kaikki tiedostot, asiakirjat tai sähköpostiviestit niiden arkaluontoisuuden mukaan. Merkintä on tehtävä Atean tietojen luokittelustandardien mukaisesti.

Tietoturvajohtajan on myös dokumentoitava ja tarkastettava kaikki henkilötietojen käsittelyrutiinit. Jokaiselle Atean esimiehelle on määritetty tietosuojaylläpitäjä (Data Protection Administrator), joka vastaa tietystä toiminteesta omassa maassaan. Tietosuojaylläpitäjän tehtävänä on varmistaa, että kaikissa hänen toiminteen liiketoimintaprosesseissa noudatetaan Atean tietosuojakäytäntöjä GDPR-asetuksen mukaisesti.

Henkilötietojen hallinta

Henkilötietoja kerätessään Atean on ilmoitettava asiasta kyseiselle henkilölle tai pyydettävä hyväksyntä tietojen keräämiseen ja käyttöön GDPR-asetuksen mukaisesti. GDPR-asetuksessa säädetään vaatimuksista, jotka liittyvät ilmoitusten sisältöön (ks. pääteksti).

Tietoturvaloukkaus tarkoittaa tilannetta, jossa luvattomat henkilöt pääsevät käsiksi tietoihin tai aiheuttavat tietojen laittoman tai tahattoman menetyksen. Atealla on GDPR:n mukaan erityisiä velvoitteita, jos henkilötietoja pääsee vuotamaan.

Kun tietoturvaloukkausta epäillään, Atean työntekijöiden on välittömästi ilmoitettava asiasta oman maansa tietoturvajohtajalle. Sähköpostia voidaan myös lähettää osoitteeseen infosec@atea.com. Tällöin, viesti välitetään suoraan Atea-konsernin tietoturvajohtajalle.

GDPR-asetuksen mukaisesti Atealla on oltava asiakkaidensa kanssa tietojenkäsittelysopimus (DPA), kun se hallinnoi asiakkaan tietoinfrastruktuuria ja sovelluksia. Atealla on oltava tietojenkäsittelysopimus myös niiden alihankkijoidensa ja toimittajiensa kanssa, jotka käsittelevät tietoa Atean puolesta tai sen lukuun. GDPR-asetuksessa säädetään vaatimuksista, jotka liittyvät tietojenkäsittelysopimuksen sisältöön (ks. pääteksti).

4. IT-INFRASTRUKTUURIN TURVALLISUUS – KAIKILTA TYÖNTEKIJÖILTÄ VAADITTAVAT TOIMENPITEET

Atean IT-infrastruktuuri koostuu laitteistosta, ohjelmistosta ja verkkokomponenteista ja niihin liittyvistä tietotekniikkaprosesseista. Nämä mahdollistavat liiketoimintajärjestelmien toteuttamisen käyttäjille. Tietosuojan toteutuminen Atealla edellyttää, että kaikki työntekijät käyttävät Atean IT-infrastruktuuria vastuullisesti.

Seuraavat käytännöt koskevat kaikkia Atean työntekijöitä Atean IT-infrastruktuurin käyttäjinä. Käytännöt kattavat laitteiden turvallisuuden, järjestelmien käytön, tiedostojen tallennuksen, verkon turvallisuuden, viestinnän ja tilaturvallisuuden. Lisäksi Atean tietotekniikkajärjestelmien hallinnoinnista vastaavien työntekijöiden on osallistuttava erilliseen laajempaan IT-turvallisuutta käsittelevään koulutukseen.

Laitteiden turvallisuus:
Atean työntekijöiden tulee noudattaa varovaisuutta päätelaitteiden, kuten tietokoneiden, tablettien ja älypuhelimien, kanssa. Nämä laitteet ovat alttiita varkauksille, haittaohjelmille ja luvattomalle käytölle. Atean tietokoneita, tabletteja ja älypuhelimia tulisi aina valvoa tai säilyttää turvallisessa paikassa. Kun näitä laitteita ei käytetä, ne on lukittava PIN-/salasanasuojauksella tai suljettava.

Kaikissa Atean tietokoneissa, tableteissa ja älypuhelimissa tulee käyttää salausratkaisuja, jotka estävät luvattoman pääsyn kiintolevylle. Atean Windows-tietokoneet aktivoidaan Bitlocker-salausratkaisulla. Apple Mac -malleissa on kiintolevyn salaamiseen sisäänrakennettu toiminto, joka on aktivoitava. Kaikki iPhone ja iPad laitteet on esiasennettu salauksella. Salaus on aktivoitava erikseen Android-puhelimissa ja tableteissa. Salaus on aktivoitava myös siirtomedioihin, kuten USB-tikkuihin, jotka voivat helposti kadota. Työntekijät, jotka tarvitsevat tukea salaukseen, voivat ottaa yhteyttä Atean palvelupisteeseen.

Atean työntekijöiden ei pitäisi ladata tietokoneisiinsa ohjelmistoja, jotka eivät ole Atean IT-osaston hyväksymiä. Atean IT-osasto tarjoaa valikoiman ohjelmistosovelluksia Acceleratorportaalin kautta. Näitä sovelluksia päivitetään säännöllisesti turvallisuustason säilyttämiseksi. Jos Atean työntekijän on ladattava tietokoneeseensa ulkoinen ohjelmisto, joka ei ole peräisin Acceleratorportaalista, hänen on ensin saatava hyväksyntä esimieheltään ja paikalliselta IT-osastolta.

Atean tietokoneisiin on asennettu valmiiksi haittaohjelmien torjunta- ja palomuurisovellukset. Jos sinulla on epäilyksiä haittaohjelmien torjuntasovelluksesta, ota yhteyttä Atean palvelupisteeseen. Jos sovellus hälyttää haittaohjelmasta tai jos tietokone toimii epänormaalisti, se voi olla merkki siitä, että tietokone on joutunut vaaraan. Tietokoneessa esiintyvien haittaohjelmien merkkejä voivat olla säännöllinen hidastuminen, epätavallisen hidas toiminta tai käyttäjän valtuuttamattomat toiminnot, kuten ponnahdusikkunat tai muut näytön muutokset.

Jos epäilet, että tietokoneesi on vaarantunut, lopeta ensin kaikki työt ja irrota tietokone verkosta. Ota sitten yhteyttä Atean palvelupisteeseen ja kuvaile, minkä perusteella epäilet haittaohjelmaa. Kerro myös mitkä seikat ovat voineet johtaa tietokoneen vaarantumiseen.

Käytöstä poistettavista työvälineistä on tyhjennettävä kaikki tiedot ennen kuin ne lähetetään Atean toimistolta huoltoa, kierrätystä tai uudelleenkäyttöä varten. Tämä on tehtävä kussakin maassa noudatettujen IT-menettelyjen mukaisesti. Nämä prosessit ovat saatavilla kunkin maan intranetin Global Information Security-sivulla.

Järjestelmän käyttö:
Atean työntekijöille on sallittava pääsy vain niihin järjestelmiin, joita he tarvitsevat työssään. Järjestelmien käyttöoikeuksia valvotaan jatkuvasti, jotta ohjeistuksen mukainen käyttöoikeuksienhallinta toteutuu. Käyttöoikeus lopetetaan heti, kun sitä ei enää tarvita. Jos Atea työntekijällä on pääsy järjestelmiin, joita hän ei enää tarvitse, hänen tulee ottaa välittömästi yhteyttä järjestelmän omistajaan käyttöoikeuksien lopettamiseksi.

Kun Atean työntekijälle myönnetään käyttöoikeudet järjestelmään, käyttäjänimi ja väliaikainen salasana annetaan erikseen. Väliaikainen salasana on vaihdettava välittömästi ensimmäisen kirjautumisen jälkeen, eikä sitä saa kirjoittaa muistiin tai jakaa kenenkään kanssa. Työntekijät eivät saa luovuttaa käyttöoikeuksiaan muille käyttäjille.

Tiedostojen tallentaminen:
Kaikki Atean työntekijät ovat vastuussa siitä, että heidän työhön liittyviä tiedostojaan (esim. MS Word/Excel/Powerpoint -tiedostot) operoidaan turvallisesti. Kaikentyyppiset tiedostot on

tallennettava Atean sisäisiin tiedostopalvelimiin, OneDrive-tileille tai Sharepoint-ympäristöön. Muita tallennuspaikkoja, mukaan lukien Dropbox tai Google Drive, ei saa käyttää Atean tiedostojen tallentamiseen ilman IT-osaston nimenomaista lupaa, koska Atea ei voi taata näiden tallennuspaikkojen turvallisuutta. Atean työntekijät eivät saa tallentaa yritystietoja paikallisiin laitteisiin, sillä tietoja ei automaattisesti varmuuskopioida, minkä vuoksi tietojen menetyksen riski on olemassa.

Tiedostot on merkittävä Atean tietojen luokit telua koskevien vaatimusten mukaisesti (5 tasoa). Ehdottoman luottamuksellisiksi merkityt tiedostot on tallennettava salatussa muodossa. Myös henkilötietoja sisältävät tiedostot on merkittävä GDPR-asetuksen mukaisesti.

GDPR-asetuksen tiukkojen henkilötietojen tallennusta koskevien vaatimusten vuoksi, Atean työntekijöiden on oltava erityisen varovaisia tallentaessaan henkilötietoja sisältäviä tiedostoja. Työntekijät eivät saa käyttää henkilötietoja muuhun kuin alkuperäiseen tarkoitukseen, joka on määritelty ja ilmoitettu sille henkilölle, jolta tiedot on kerätty. Työntekijöiden on rajoitettava henkilötietojen jakamista väärinkäytön estämiseksi. Henkilötiedot on poistettava heti, kun niitä ei enää tarvita. Tämä koskee kaikkia Atean työntekijöiden luomia tiedostoja, kuten MS Word/ Excel/Powerpoint-tiedostoja.

Verkkoturvallisuus:

Vain Atean määrittelemät päätelaitteet (Atean standardien mukaan konfiguroidut tietokoneet) saavat muodostaa yhteyden ATEA-toimialueeseen. Atean mobiililaitteilla ja tietokoneilla saa muodostaa yhteyden vain niille tarkoitettuun Atean WiFi-verkkoon. Muut tietokoneet tai mobiililaitteet yhdistetään Atea-vieras WiFi -verkkoon.

Atea tarjoaa toimiston ulkopuolella oleville työntekijöille mahdollisuuden muodostaa etäyhteyden sisäiseen verkkoon Cisco VPN tai Citrix-ohjelmiston kautta. Cisco VPN -yhteys edellyttää, että tietokone kuuluu Atealle ja on liitetty Atean toimialueeseen (ONE) sekä siihen on asennettu haittaohjelmien torjuntasovellus.

Atean työntekijät eivät saa koskaan muodostaa yhteyttä asiakkaan verkkoon ilman asiakkaan etukäteen antamaa suostumusta, ellei asiakassopimuksessa toisin määrätä. Asiakkaaseen tulee ottaa yhteyttä aina, kun Atean työntekijä muodostaa yhteyden asiakkaan verkkoon. Ellei toisin sovita, Atean työntekijän on ilmoitettava asiakkaalle, mitä hän on tehnyt asiakkaan verkossa.

Atean työntekijöiden tulee olla varovaisia käyttäessään matkoilla julkisia WiFi-verkkoja. Tietoliikennettä julkisissa verkoissa voidaan seurata. Ennen WiFi-verkon käyttöä Atean työntekijöiden tulee huolehtia siitä, että verkko on suojattu ja peräisin asialliselta taholta. Jos yleisen WiFi-verkon turvallisuutta on syytä epäillä, Atean työntekijän tulisi sen sijaan käyttää omaa mobiiliverkkoa. Atean palvelupiste voi auttaa tietokoneen liittämisessä mobiiliverkkoon.

Atean työntekijöiden odotetaan käyttävän internetiä päivittäisessä työssään. Yksityinen selailu on sallittua, mutta sen tulee rajoittua sivustoihin, joiden sisältö sopii työpaikalle. Verkkopelaaminen tai uhkapelit eivät ole sallittuja, ja tiedostojen jakaminen tai median suoratoisto internetin kautta on rajoitettava työhön liittyvään sisältöön.

Kaikkien työntekijöiden tulee olla tietoisia siitä, että Atea analysoi internetin kautta tapahtuvaa liikennettä Ateaa vastaan tehtyjen hyökkäysten havaitsemiseksi. Analyysitoiminta seuraa myös internetin väärää käyttöä.

Kun käytät internet-sivuja, ole varovainen – varsinkin jos sinut ohjataan sinne toiselta sivulta. Älä koskaan käynnistä verkkosivuilla olevia linkkejä tai ponnahdusikkunoita, jos ne näyttävät epäilyttäviltä. Ne voivat sisältää haittaohjelmia, jotka voidaan ladata laitteeseesi.

Viestintä (sähköposti / sosiaalinen media):
Sähköposti on olennainen digitaalinen viestintäväline Atean työntekijöille. Se on myös merkittävä tietoturvan haavoittuvuuslähde, sillä se antaa hyökkääjille mahdollisuuden altistaa Atean haittaohjelmille, petoksille ja muille uhkille edullisesti ja pienellä riskillä.

Tietojen kalastelu on yksi tavallisimmista Ateaan kohdistuvista huijaustyypeistä. Siinä hyökkäävä taho ottaa yhteyttä suoraan Atean työntekijään sähköpostitse. Sähköposti näyttää olevan peräisin luotettavasta lähteestä ja lähettäjä hyödyntää usein väärennettyä identiteettiä. Hän voi esiintyä esimerkiksi Atean toisena työntekijänä, liikekumppanina tai teknologiayrityksen tai pankin edustajana. Sähköpostin on tarkoitus huijata Atean työntekijää esimerkiksi siirtämään rahaa, paljastamaan käyttäjätunnus, salasana tai muita arkaluontoisia tietoja tai käynnistämään linkin tai liitetiedoston, jolloin tietokoneelle tai mobiililaitteelle ladataan haittaohjelma.

Sähköpostiviesti, liite tai linkki näyttää viattomalta. Se on esimerkiksi naamioitu kollegan viestiksi, toimittajan tarjoukseksi/laskuksi tai ilmoitukseksi vaikkapa OneDrivesta. Tästä syystä Atean työntekijöiden on oltava varuillaan sähköposteihin ja muuhun viestintään liittyvään sisältöön, vaikka viesti vaikuttaisi tulevan luotetusta lähteestä.

Atean työntekijät eivät saa avata linkkejä tai liitetiedostoja omissa laitteissaan, jos heillä on epäilyksiä sähköpostin tai viestin alkuperästä. Jos Atean työntekijä on epävarma sähköpostin turvallisuudesta tai jos hän on vahingossa vastannut mahdolliseen hyökkäykseen avaamalla epäilyttävän linkin tai liitetiedoston, hänen tulee ottaa välittömästi yhteyttä Atean palvelupisteeseen.

Työntekijöiden sähköpostitileihin kohdistuu usein hyökkäyksiä, joissa pyritään pääsemään käsiksi työntekijän arkaluontoisiin liiketoimintatiedostoihin. Tästä syystä sähköpostia ei saa käyttää tärkeiden yritystietojen arkistointiin. Yritystietoja on säilytettävä tai jaettava suojattujen liiketoimintajärjestelmien tai tiedostojen jakamisratkaisujen avulla sähköpostin sijaan.

Sähköpostin yksityinen käyttö on sallittua, sillä edellytyksellä, että käyttö ei ole ristiriidassa Atean liiketoiminnan etujen kanssa tai häiritse työaikaa. Yksityisen sähköpostiviestinnän on aina oltava sopivaa työpaikalle, ja viesteihin on liitettävä merkintä "Non-Business", mikäli mahdollista. Lisäksi, jos yrityksen sähköpostitiliä käytetään henkilökohtaiseen viestintään, ei saa syntyä sellaista vaikutelmaa, että kirjeenvaihtoa käydään Atean nimissä.

Sosiaalinen media on myös Atean työntekijöiden usein käyttämä viestintäkanava. Kun sosiaalista mediaa käytetään oikein, se tarjoaa Atean työntekijöille mahdollisuuden hankkia ja siirtää tietoa, rakentaa liikesuhteita ja vahvistaa Atean brändiä. Toisaalta sosiaalinen media voi vahingoittaa Ateaa ja sen työntekijöitä, jos sitä käytetään väärin tai jos siellä jaetaan arkaluontoisia tietoja.

Atean työntekijöiden tulee noudattaa hyvää harkintaa sen suhteen, mitä tietoja he jakavat sosiaalisessa mediassa. Henkilötietoja (mukaan lukien nimet, valokuvat jne.) voidaan jakaa Atean liiketoimintaan liittyvissä sosiaalisen median viesteissä ainoastaan, jos henkilö, jonka tiedot jaetaan, suostuu niiden käyttöön.

Toimistojen turvallisuus:
Atean työntekijöiden on käytettävä kulkukortteja. Kaikkien Atean vierailijoiden on rekisteröidyttävä vastaanotossa, josta he saavat vierailuun tarkoitetun kulkukortin. Se on asetettava näkyvälle paikalle. Vieraat otetaan vastaan vastaanotossa vierailun alussa. Vierailun lopussa heidät saatetaan vastaanottoon, jonne he palauttavat vierailijakorttinsa. Vieraita ei saa jättää yksin Atean tiloihin.

Kaikki arkaluontoiset tiedot tulee poistaa työpöydiltä ja laittaa varmaan talteen, kun ne eivät ole käytössä. Kokousten lopussa tiedot pyyhitään pois kirjoitustauluilta. Luottamukselliset asiakirjat on aina hävitettävä silppureissa tai heitettävä niille varattuihin roskakoreihin, kun niitä ei enää tarvita.

Kertaus – IT-infrastruktuurin turvallisuus

Laitteiden turvallisuus:
Kaikissa Atean tietokoneissa, tableteissa ja älypuhelimissa tulee käyttää salausratkaisuja, jotka estävät luvattoman pääsyn tietoihin. Atean tietokoneita, tabletteja ja älypuhelimia tulisi aina valvoa tai säilyttää turvallisessa paikassa. Kun näitä laitteita ei käytetä, ne on lukittava PIN-/salasanasuojauksella tai suljettava.

Atean työntekijöiden ei pitäisi ladata tietokoneisiinsa ohjelmistoja, jotka eivät ole Atean IT-osaston hyväksymiä. Jos työntekijän on ladattava tietokoneeseensa ulkoinen ohjelmisto, joka ei ole peräisin Atealta, hänen on ensin saatava hyväksyntä esimieheltään ja paikalliselta IT-osastolta.

Atean tietokoneisiin on asennettu valmiiksi haittaohjelmien torjunta- ja palomuurisovellukset. Jos sinulla on epäilyksiä haittaohjelmien torjuntasovelluksesta, ota yhteyttä Atean palvelupisteeseen.

Jos epäilet, että tietokoneessasi on haittaohjelma tai muu haavoittuvuus, lopeta ensin kaikki työn alla olevat tehtävät ja irrota tietokone verkosta. Ota sitten yhteyttä Atean palvelupisteeseen.

Järjestelmän käyttö:
Atean työntekijöille on sallittava pääsy vain niihin järjestelmiin, joita he tarvitsevat työssään. Järjestelmien käyttöoikeuksia valvotaan jatkuvasti ja käyttöoikeus lopetetaan heti, kun sitä ei enää tarvita.

Tiedostojen tallennus:
Kaikki Atean työntekijät ovat vastuussa siitä, että heidän työhön liittyviä tiedostoja (esim. MS Word/Excel/Powerpoint -tiedostot) hoidetaan turvallisesti. Tiedostot on merkittävä Atean tietojen luokittelua koskevien vaatimusten (5 tason) mukaisesti, ja henkilötietoja sisältävät tiedostot on merkittävä erikseen. Ehdottoman luottamuksellisiksi merkityt tiedostot on tallennettava salatussa muodossa.

Kaikentyyppiset tiedostot on tallennettava Atean sisäisiin tiedostopalvelimiin, OneDrive-tileille tai Sharepoint-ympäristöön. Muita tallennuspaikkoja, mukaan lukien Dropbox tai Google Drive, ei saa käyttää Atean tiedostojen tallentamiseen ilman IT-osaston nimenomaista lupaa. Atean työntekijät eivät saa tallentaa yritystietoja paikallisille laitteille.

Verkkoturvallisuus:
Vain Atean määrittelemät päätelaitteet (Atean standardien mukaan konfiguroidut tietokoneet) saavat muodostaa yhteyden ATEA-toimialueeseen. Atean mobiililaitteilla ja tietokoneilla saa muodostaa yhteyden vain niille tarkoitettuun Atean WiFi-verkkoon. Muut tietokoneet tai mobiililaitteet voivat käyttää ATEA-vieraiden WiFi-verkkoa.

Atean työntekijöiden tulee olla varovaisia käyttäessään julkisia WiFi-verkkoja. Ennen WiFi-verkon käyttöä Atean työntekijöiden tulee varmistaa, että verkko on suojattu ja peräisin asialliselta tarjoajalta.

Internetin käyttö työkoneella on sallittua, mutta se tulee rajoittaa sivustoihin, joiden sisältö sopii työpaikalle. Kaikkien työntekijöiden tulisi olla tietoisia siitä, että Atea analysoi internetin kautta tapahtuvaa liikennettä Ateaa vastaan tehtyjen hyökkäysten havaitsemiseksi. Analyysitoiminta seuraa myös internetin väärää käyttöä.

Kun käytät verkkosivuja, ole varovainen – varsinkin jos sinut ohjataan sinne toiselta sivulta. Älä koskaan käynnistä verkkosivuilla olevia linkkejä tai ponnahdusikkunoita, jos ne näyttävät epäilyttäviltä. Ne voivat sisältää haittaohjelmia, jotka voidaan ladata laitteeseesi.

Viestintä (sähköposti / sosiaalinen media):
Sähköposti on merkittävä tietoturvan haavoittuvuuslähde, sillä se antaa hyökkääjille mahdollisuuden altistaa Atea haittaohjelmille, petoksille ja muille uhkille edullisesti ja pienellä riskillä.

Tietojen kalastelu on yksi tavallisimmista Ateaan kohdistuvista huijaustyypeistä. Siinä rikollinen ottaa yhteyttä suoraan Atean työntekijään sähköpostitse. Sähköposti näyttää olevan peräisin luotettavasta lähteestä ja lähettäjä hyödyntää usein väärennettyä identiteettiä. Hän voi esiintyä esimerkiksi Atean toisena työntekijänä, liikekumppanina tai teknologiayrityksen tai pankin edustajana. Sähköpostin on tarkoitus huijata Atean työntekijää esimerkiksi siirtämään rahaa, paljastamaan käyttäjätunnus, salasana tai muita arkaluontoisia tietoja tai käynnistämään linkki tai liitetiedosto, jolloin tietokoneelle tai mobiililaitteelle ladataan haittaohjelma.

Atean työntekijät eivät saa avata linkkejä tai liitetiedostoja omissa laitteissaan, jos heillä on epäilyksiä sähköpostin tai viestin alkuperästä. Jos Atean työntekijä on epävarma sähköpostin turvallisuudesta tai jos hän on vahingossa vastannut mahdolliseen huijausyritykseen avaamalla epäilyttävän linkin tai liitetiedoston, hänen tulee ottaa välittömästi yhteyttä Atean palvelupisteeseen.

Sähköpostin yksityinen käyttö on sallittua, sillä edellytyksellä, että käyttö ei ole ristiriidassa Atean liiketoiminnan etujen kanssa tai häiritse työaikaa. Yksityisen sähköpostiviestinnän on aina oltava sopivaa työpaikalle, ja viestiin on liitettävä merkintä ”Non-Business”, mikäli mahdollista.

Atean työntekijöiden on noudatettava harkintaa sen suhteen, mitä tietoja he jakavat Ateasta sosiaalisessa mediassa. Henkilötietoja (mukaan lukien nimet, valokuvat jne.) voidaan jakaa Ateaan liittyvissä sosiaalisen median viesteissä ainoastaan, jos henkilö, jonka tiedot jaetaan, suostuu niiden käyttöön.

Toimistojen turvallisuus:
Atean työntekijöiden on käytettävä kulkukortteja. Kaikkien Atean vierailijoiden on rekisteröidyttävä vastaanotossa, josta he saavat vierailuun soveltuvan kulkukortin. Se asetetaan näkyvälle paikalle.

Kaikki arkaluontoiset tiedot otetaan pois työpöydiltä ja laitetaan varmaan talteen, kun ne eivät ole käytössä.

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

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

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

Tanska
Atea A/S
Lautrupvang 6
DK-2750 Ballerup
+45 70 25 25 50
Y-tunnus 25511484
info@atea.dk
atea.dk

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

Liettua
Atea Baltic UAB
J. Rutkausko st. 6
LT-05132 Vilnius
+370 5 239 7899
Y-tunnus 300125003
info@atea.lt
atea.lt

Konsernin logistiikka
Atea Logistics AB
Smedjegatan 12
Box 159
SE-351 04 Växjö, Sweden
+46 (0)470 77 16 00
Y-tunnus 556354-4690
customer.care@atea.se

Konsernin yhteiset palvelut
Atea Global Services SIA
Mukusalas Street 15
LV-1004 Riga, Latvia
+371 67359600
Y-tunnus 50203101431
rigainfo@atea.com
ateaglobal.com

ATEA