TP2B THE PLACE TO BE

ATEA

INFORMACIJOS SAUGUMO RIZIKOS VALDYMAS: DARBUOTOJŲ POLITIKA

1.0 versija – paskelbta 2019 m. rugpjūčio mėn.

GENERALINIO DIREKTORIAUS LAIŠKAS

„Atea“ misija yra „kurti ateitį su IT“.

Mes tikime, kad informacinės technologijos, kartu su žiniomis ir kūrybiškumu, gali transformuoti našumą ir kelti visos visuomenės gyvenimo lygį. Mes padedame privačioms ir viešojo sektoriaus įmonėms bei organizacijoms kurti skaitmeninius sprendimus, leidžiančius joms pasiekti geresnių, efektyvesnių rezultatų, panaudojant mažiau išteklių.

Tuo pat metu mes suprantame rizikas, būdingas technologijoms, kuomet kaupiama ir apdorojama vis daugiau informacijos. Kadangi organizacijose tvarkoma vis daugiau duomenų, o procesai IT sistemose ir tinkluose automatizuojami, nuolat didėja kibernetinių atakų grėsmė dėl duomenų vagystės, tapatybės sukčiavimo ar veiklos sutrikimų. Duomenų pažeidimo atveju, asmens duomenys gali tapti pasiekiami be asmens sutikimo, tokiu būdu pakenkiant asmeniui ir pažeidžiant jo teisę į privatumą.

„Atea“ yra pirmaujanti informacinių technologijų teikėja Skandinavijos ir Pabaltijo regionuose, todėl ji turi ypatingą pareigą užtikrinti, kad įmonių grupės veikla atitiktų griežtus informacijos saugumo standartus. „Atea“ projektuoja, diegia ir prižiūri didžiausių ir svarbiausių mūsų regionų organizacijų IT infrastruktūros sprendimus. Didžioji mūsų pardavimų dalis tenka valstybinėms ir vietos valdžios institucijoms, įskaitant ypatingus klientus, tokius kaip kariuomenė ar policija. Mes taip pat teikiame kritiškai svarbius IT sprendimus didelėms įmonėms savo regionuose.

Šis dokumentas yra Atea informacijos saugumo rizikų valdymo vadovas. Jame pateikiamos pagrindinės saugumo rizikos, duomenų apsaugos politika ir valdymo procedūros, turinčios įtakos visiems mūsų įmonėje. Darbuotojai, atsakingi už IT eksploatavimą ir sistemų administravimą, turės atlikti atskirus, išsamesnius žinių patikrinimus informacijos saugumo ir duomenų apsaugos politikos klausimais, kaip to reikalauja jų darbo funkcijos.

Šis dokumentas yra sudarytas iš keturių dalių, kiekvienos pabaigoje pateikiant apibendrinimus – svarbiausius akcentus. Kadangi informacijos sauga yra itin svarbi tema verslo požiūriu, visuose skyriuose pateikiama išsami informacija. Ypač svarbu, kad darbuotojai įsidėmėtų kiekvieno skyriaus pabaigoje pateiktus akcentus ir prireikus galėtų prisiminti informaciją likusioje dokumento dalyje.

Visi „Atea“ darbuotojai privalo žinoti šio dokumento turinį. Siekiant užtikrinti, kad visi „Atea“ darbuotojai suprastų šio dokumento turinį, Elgesio kodekso žinių patikrinimas, kuris yra privalomas visiems „Atea“ darbuotojams, papildytas dešimčia klausimų, susijusių su informacijos sauga. Darbuotojams yra parengtas ir internetinis mokymo kursas, padėsiantis labiau įsigilinti į „Atea“ informacijos saugumo politiką ir pasirengti Elgesio kodekso žinių patikrinimui.

„Atea“ yra didelė organizacija, veikianti septyniose šalyse ir turinti 90 biurų. „Atea“ grupei informacijos saugos srityje vadovauja vyriausiasis informacijos apsaugos pareigūnas (Group CISO), o kiekvienoje šalyje ar verslo vienetuose (kaip pvz. „Atea Baltic“) paskirti jam pavaldūs lokalūs vyriausieji informacijos apsaugos

Steinar Sønsteby,
Generalinis direktorius

pareigūnai (CISO), kurie kontroliuoja informacijos saugumo politikos įgyvendinimą visoje „Atea“ grupėje.

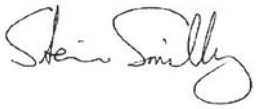
Jei turite klausimų ar nusiskundimų dėl informacijos saugumo „Atea“, prašome kreiptis atitinkamai pagal sritis, įvardintas žemiau:

- Jei nerimaujate, kad Jūsų kompiuteris gali būti užkrėstas kenkėjiškomis programomis arba turite bendro pobūdžio klausimų, susijusių su IT saugumu, kreipkitės į „Atea“ Servicedesk.
- Norėdami pranešti apie įtartiną el. laišką, bandymą sukčiauti ar kitą įvykį, galintį kelti „Atea“ informacijos saugumo riziką, kreipkitės į „Atea“ Servicedesk.
- Jei norite pranešti apie įtariamą asmens ar verslo duomenų pažeidimą (neteisėtą atskleidimą) iš informacinių sistemų ar dokumentų, kreipkitės į šalies, kurioje dirbate, vyriausiąjį informacijos apsaugos pareigūną (CISO). Taip pat galite siųsti laišką tiesiai į infosec@atea.com.

Jei norite tiesiogiai susisiekti su „Atea“ grupės vyriausiuoju informacijos apsaugos pareigūnu (Group CISO), savo šalies ar verslo vieneto vyriausiuoju informacijos apsaugos pareigūnu (CISO), jų kontaktus rasite „Atea“ internetiniame puslapyje: atea.com/trust. Visi laiškai, siunčiami į infosec@atea.com, bus persiųsti „Atea“ grupės vyriausiajam informacijos apsaugos pareigūnui (Group CISO).

Mes džiaugiamės galėdami gauti Jūsų klausimus bei atsiliepimus ir pažadame, kad nesiimsime jokių atsakomųjų veiksmų, susijusių su Jūsų pranešimais. Tačiau jei norite anonimiškai pranešti apie problemas, galite pateikti informaciją „Atea“ atvirumo linija. Nuorodą į šią liniją taip pat galite rasti „Atea“ internetiniame puslapyje: atea.com/trust. Visi pranešimai, gauti atvirumo linija, siunčiami nepriklausomai advokatų kontorai, kuri apibendrina ir pateikia informaciją atitinkamam „Atea“ organizacijos lygmeniui.

Griežtų informacijos saugumo standartų laikymasis yra būtinas „Atea“ vykdant veiklą ir dirbant su klientais ir partneriais, bei svarbiausiais IT iššūkiais Skandinavijos ir Pabaltijo regionuose. Dėkojame, kad vadovaujatės „Atea“ informacijos saugumo politika ir kad esate „The Place to Be” dalis.



Svarbiausi akcentai:

„Atea“ labai svarbu, kad visi darbuotojai laikytųsi griežtų informacijos saugumo standartų.

Grupei ir kiekvienai šaliai ar verslo vienetui yra paskirtas vyriausiasis informacijos apsaugos pareigūnas (CISO), kuris kontroliuoja informacijos saugumo politikos įgyvendinimą visoje „Atea“. Vyriausiųjų informacijos apsaugos pareigūnų vardai ir pavardės yra pateikti „Atea“ internetiniame puslapyje atea.com/trust.

Jei turite klausimų ar nusiskundimų dėl informacijos saugumo „Atea“, prašome kreiptis atitinkamai pagal sritis, įvardintas žemiau:

- Jei nerimaujate, kad Jūsų kompiuteris gali būti užkrėstas kenkėjiškomis programomis arba turite bendro pobūdžio klausimų, susijusių su IT saugumu, kreipkitės į „Atea“ Servicedesk;
- Norėdami pranešti apie įtartiną el. laišką, bandymą sukčiauti ar kitą įvykį, galintį kelti „Atea“ informacijos saugumo riziką, kreipkitės į „Atea“ Servicedesk;
- Jei norite pranešti apie įtariamą asmens ar verslo duomenų pažeidimą (neteisėtą atskleidimą) iš informacinių sistemų ar dokumentų, kreipkitės į šalies, kurioje dirbate, vyriausiąjį informacijos apsaugos pareigūną (CISO). Taip pat galite siųsti laišką tiesiai infosec@atea.com.

Turinys

1. INFORMACIJOS SAUGUMAS: APŽVALGA IR RIZIKOS VALDYMAS

Informacija yra svarbi bet kurios organizacijos veiklai. Informacijos saugumo valdymo sistema (ISMS) yra politikos, procedūrų, įrankių ir veiklos, kurią organizacija naudoja savo informacijos turtui apsaugoti nuo neleistinos prieigos ir netinkamo naudojimo, rinkinys.

Norint sukurti informacijos saugumo valdymo sistemą, reikia, kad organizacija identifikuotų savo turimą informaciją. Tai apima visus duomenis, kuriuos organizacija tvarko, nepriklausomai nuo jų formos: skaitmeniniu būdu, popieriuje arba žodžiu. „Atea“ ši informacija gali būti skirta vidaus naudojimui arba tai gali būti išoriniai duomenys, kuriuos „Atea“ valdo ir apdoroja teikdama paslaugas savo klientams.

Informacijos saugumo valdymo sistemos paskirtis – apsaugoti ir išsaugoti informacinio turto konfidencialumą, vientisumą ir prieinamumą.

- **Konfidencialumas** reiškia, kad informacija gali būti prieinama tik įgaliotiems asmenims.
- **Vientisumas** reiškia, kad informacija tvarkoma taip, kad ji būtų pilna ir tiksli.
- **Prieinamumas** reiškia, kad įgalioti asmenys gali pasiekti ir naudoti duomenis, kai to reikia.

Siekdama šių tikslų, organizacija turi atlikti rizikos vertinimą ir identifikuoti, kaip jos informacinis turtas gali būti paveiktas atsižvelgiant į potencialias informacijos saugumo grėsmes. Tuomet ji gali sukurti informacijos saugumo valdymo sistemą, kuri padėtų veiksmingai valdyti ir kontroliuoti šias rizikas be bereikalingų išlaidų ar veiklos našumo praradimo.

„Atea“ rizikos vertinimas

Kaip „Atea“ verslo prioritetai, nustatytos šios svarbiausios informacijos saugumo rizikos:

1. **Fiziniai nuostoliai:**
   Informacinis turtas saugomas fiziniuose įrenginiuose, kurie gali būti prarasti, pavogti ar sugadinti. Prieigos valdymas, šifravimas ir duomenų atsarginių kopijų darymas yra būtini, norint sumažinti galimą riziką, susijusią su fiziniu turtu (pvz., kompiuteriais, mobiliaisiais telefonais, serveriais ir saugyklomis). Duomenų centrai yra ypač pažeidžiami ir turi būti apsaugoti nuo aplinkos pavojų, įskaitant temperatūrą ir gaisrą.
2. **Tapatybės sukčiavimas:**
   „Atea“ nuolatos susiduria su sukčiavimo bandymais, kurių metu naudojama netikra tapatybė ar apgaulė siekiant pasinaudoti darbuotojo pasitikėjimu. Tokių bandymų tikslas paprastai yra pavogti iš „Atea“ duomenis arba gauti neteisėtą prieigą prie „Atea“ sistemų ir tinklų.

   Viena iš „Atea“ tapatybės sukčiavimo rūšių yra netikrų ar pavogtų klientų sąskaitų duomenų naudojimas siekiant užsakyti IT įrangą, ypač per „Atea Eshop“. Be „Eshop“ prieigos kontrolės, „Atea“ turi verslo procedūras, kuriomis siekiama peržiūrėti naujų klientų paskyras ir nustatyti neįprastą klientų veiklą, kad būtų sumažinta nesąžiningų klientų sandorių rizika.

   Dar vienas labai dažnas tapatybės sukčiavimo „Atea“ atvejis („phishing“), kai sukčius tiesiogiai kreipiasi į „Atea“ darbuotoją. El. laiškas atrodo tarsi būtų siųstas iš patikimo šaltinio, dažnai naudojant netikrą tapatybę, pvz., kito „Atea“ darbuotojo, verslo partnerio ar tiekėjo (pvz., technologijų įmonės ar banko). El. laišku bandoma paveikti„Atea“ darbuotoją, kad jis atliktų laiške nurodytus veiksmus, pvz., pervestų pinigus, įvestų prisijungimo / slaptažodžio duomenis ar kitą slaptą informaciją, arba paspaustų nuorodą ar atidarytų priedą, kuris parsiunčia kenkėjišką programinę įrangą („malware“) į vartotojo kompiuterį ar mobilųjį telefoną.

   Laiškas, jo priedas ar nuoroda gali atrodyti nekaltai – pavyzdžiui, bus užmaskuotas kaip kolegos laiškas, tiekėjo pasiūlymas, sąskaita faktūra arba kaip debesijos paskyros, pvz., „OneDrive“, pranešimas. Dėl šios priežasties „Atea“ darbuotojai turi būti labai budrūs tvarkydami el. laiškus ar kitokio pobūdžio pranešimus, net jei jie atrodo gauti iš patikimo šaltinio.

   „Atea“ darbuotojai turi neatidaryti nuorodų arba priedų iš savo prietaisų, jei jie abejoja elektroninio laiško ar kitokio kontakto su juo teisėtumu. Jei „Atea“ darbuotojas nėra tikras dėl elektroninio laiško teisėtumo arba jei

netyčia sureagavo į galimą mėginimą sukčiauti, atidaręs įtartiną nuorodą ar priedą, jis turi nedelsdamas kreiptis į „Atea“ Servicedesk ir pranešti apie incidentą.

Nors elektroninis paštas yra labiausiai paplitęs sukčiavimo būdas, „Atea“ darbuotojai taip pat turėtų būti budrūs ir stebėti kitas apgaulingų ryšių formas, įskaitant telefonines užklausas arba kvietimus į socialinės žiniasklaidos priemones.

3. Verslo paslapčių vagystė:

Jei neįgalioti asmenys gauna prieigą prie „Atea“ informacinių sistemų, jie gali bandyti pavogti intelektine nuosavybe laikomą informaciją, kuri yra svarbi „Atea“ veiklai. Tai gali apimti slaptą verslo informaciją, pvz., kliento ar tiekėjo duomenis, sutartis ir komercines sąlygas. Tai taip pat gali apimti intelektinę nuosavybę, pavyzdžiui, verslo koncepcijas, produktų ar paslaugų dizainą ir įmonės sukurtą programinę įrangą, metodikas ir priemones.

Darbuotojai, turintys prieigą prie pagrindinių sistemų, taip pat gali bandyti pavogti „Atea“ verslo paslaptis, ypač jei jie planuoja išeiti iš įmonės. Siekiant sumažinti riziką, prieiga prie informacijos turi būti suteikta tik tiems darbuotojams, kuriems ji reikalinga darbinėms funkcijoms atlikti. Sistemos prieiga turėtų būti nuolat tikrinama, siekiant užtikrinti, kad laikomasi principo „būtina žinoti“, ir kad naudotojo prieigos teisės panaikinamos, kai jos tampa nebereikalingos.

Be prieigos kontrolės, „Atea“ dar naudoja saugos informacijos ir įvykių valdymo (SIEM) įrankius, skirtus analizuoti įvykių žurnalų („log“) informaciją ir tai, kokie veiksmai įvyko jos sistemose.

4. Verslo veiklos sutrikdymas:

„Atea“ veikla priklauso nuo IT sistemų. Jei pažeidžiama prieigos kontrolė arba jei sistemos netinkamai naudojamos, gali būti nutekinta asmeninė darbuotojų ar verslo partnerių informacija. Informacija, kuri reikalinga „Atea“ verslui vykdyti, gali būti sugadinta arba ištrinta. Galiausiai, verslo sandorius gali įvesti arba patvirtinti pašaliniai asmenys, pažeisdami „Atea“ valdymo kontrolę. Visi šie įvykiai yra pavojingi „Atea“ verslo veiklai.

Taip pat yra pavojus, kad „Atea“ veiklą gali sutrikdyti sudėtinga įsilaužimo ataka, kuri išjungs pagrindines IT sistemas ar tinklus. Sistemos gali būti užkrėstos kenkėjiškomis programomis, kurios neleidžia vartotojams naudotis svarbiausiomis sistemų funkcijomis arba nuskaityti duomenų failus, nebent būtų sumokėta išpirka („ransomware“). Tinklai ar serveriai gali būti užtvindyti srautu ar užklausomis taip, kad jie nebegalės vykdyti teisėtų operacijų („paslaugų trikdymo“ atakos). Šie išpuoliai gali būti nukreipti į „Atea“ arba klientus, kuriuos „Atea“ valdo iš savo duomenų centro.

5. Sutartinės žalos atlyginimas:

„Atea“ turi konfidencialumo susitarimus su daugeliu klientų, pardavėjų ir verslo partnerių. „Atea“ taip pat turi paslaugų lygio susitarimus („service level agreements“, SLA) ir duomenų tvarkymo sutartis (DPA) su klientais, kurie naudojasi „Atea“ IT paslaugomis ir palaikymo paslaugomis.

IT saugumo incidentas „Atea“ gali pažeisti konfidencialumo, paslaugų lygio ir duomenų tvarkymo sutartis su klientais ir kitais verslo partneriais. Dėl to jie gali iškelti ieškinius „Atea“ dėl žalos, patirtos dėl sutarčių pažeidimo, atlyginimo. Be tiesioginių nuostolių, IT saugumo incidentas gali sukelti ilgalaikę žalą „Atea“ verslo santykiams su klientais ir partneriais.

Net tais atvejais, kai „Atea“ neturi konkrečios sutarties, „Atea“ gali susidurti su įmonių ar asmenų teisiniais reikalavimais, jei jų duomenys bus pavogti ar netinkamai panaudoti ir „Atea“ neįrodys taikanti pakankamas informacijos saugos priemones tvarkant duomenis.

6. Teisinės sankcijos:

Kaip „Oslo“ vertybinių popierių biržoje kotiruojama bendrovė, „Atea“ privalo laikytis griežtų teisinių reikalavimų tvarkydama duomenis, kurie nėra žinomi rinkoje ir kurie gali turėti įtakos jos akcijų kainai („neskelbtina informacija apie kainas“). Tai gali apimti informaciją apie pagrindines naujas sutartis arba finansinius rezultatus, apie kuriuos dar nebuvo pranešta viešai.

„Atea“ turi konfidencialiai tvarkyti neskelbtiną informaciją apie kainas siekiant užtikrinti, kad ši informacija būtų prieinama tik ribotam

skaičiui registruotų vidinių asmenų, laikantis principo „būtina žinoti“. Darbuotojai, turintys neskelbtinos informacijos apie kainas, turi būti registruojami įmonėje ir jiems taikomi specialūs reikalavimai dėl informacijos neatskleidimo ir apribojimai prekiauti „Atea“ akcijomis. Už šių teisinių reikalavimų pažeidimą darbuotojas gali būti patrauktas baudžiamojon ir teisinėn atsakomybėn pagal Norvegijos vertybinių popierių prekybos įstatymą.

„Atea“ taip pat gali būti taikomos sankcijos ir nuobaudos už duomenų pažeidimą, susijusį su asmens duomenimis pagal Europos Sąjungos Bendrąjį duomenų apsaugos reglamentą (BDAR). Kadangi BDAR reikalavimai yra gana plati tema, informacija apie tai pateikiama atskirame šio dokumento skyriuje apie duomenų privatumą.

Pagrindiniai akcentai:

Visi darbuotojai turi būti labai atsargūs tvarkydami informaciją ir dirbdami su IT sistemomis, kad išvengtų saugumo pažeidimų.

IT įranga gali būti prarasta, pavogta ar sugadinta. Todėl norint sumažinti galimą informacijos saugumo riziką, būtina naudotis prieigos kontrole, šifravimu ir duomenų atsarginių kopijų kūrimu.

„Atea“ nuolatos susiduria su sukčiavimo bandymais, kurių metu naudojama netikra tapatybė ar apgaulė siekiant pasinaudoti darbuotojo pasitikėjimu. Atkreipkite dėmesį, kad bet koks Jūsų gautas el. laiškas ar kitu būdu gauta informacija gali būti bandymas sukčiauti, net jei atrodo, kad jis atėjo iš teisėto šaltinio (įskaitant pranešimą iš „Atea“ vadovo, kliento, technologijų tiekėjo ar socialinės žiniasklaidos paskyros).

Būkite atidūs esant bet kokiam neįprastam kontaktui su Jumis ar veiklai. Jei įtariate bandymą sukčiauti el. paštu ar kito tipo pranešimu, kreipkitės į „Atea“ Servicedesk. Neatlikite jokių įtartinuose pranešimuose įvardintų veiksmų, pvz., neatidarykite el. laiško priedų ir išorinių nuorodų, nevykdykite užsakymų ir mokėjimų.

Siekiant sumažinti informacijos vagystės ar netinkamo naudojimo riziką, prieiga prie informacijos turi būti suteikta tik darbuotojams, kuriems jos reikia darbinėms funkcijoms atlikti. Sistemos prieiga turėtų būti nuolat tikrinama, siekiant užtikrinti, kad vartotojo prieigos teisės būtų panaikintos, kai jų nebereikia.

Dėl informacijos saugumo incidento gali būti padaryta didelė žala „Atea“, nes sutrinka jos verslo procesai, pažeidžiamos „Atea“ sutartinės prievolės klientams ir verslo partneriams, taikomos sankcijos ir kyla žala „Atea“ reputacijai bei verslo santykiams.

2. DUOMENŲ PRIVATUMAS: APŽVALGA IR RIZIKOS VALDYMAS

Duomenų privatumas apima asmens kontrolę savo duomenų atžvilgiu, o konkrečiai – gebėjimą nustatyti, kada ir kaip renkami, bendrinami ir naudojami jo duomenys. Asmens duomenys apibrėžiami kaip bet kokia informacija, kurią galima susieti su konkrečiu ir identifikuojamu asmeniu.

Duomenų privatumas priklauso nuo informacijos saugumo, t. y. kaip duomenys yra apsaugoti nuo neteisėtos prieigos ir netinkamo naudojimo. Tačiau duomenų privatumas apima ne tik informacijos saugumą, bet ir asmens teisių į savo duomenis apsaugą. Konkrečiai – kaip organizacija kiekvienam asmeniui suteikia galimybę kontroliuoti savo asmens duomenų naudojimą, kai organizacija renka ir apdoroja informaciją apie tą asmenį.

„Atea“ tvarko asmens duomenis laikydamasi duomenų privatumo kaip pagrindinės žmogaus teisės. „Atea“ taikomi griežti teisiniai reikalavimai tvarkant asmens duomenis, kaip apibrėžta Europos Sąjungos Bendrajame duomenų apsaugos reglamente (BDAR).

„Atea“ taikomus BDAR reikalavimus galima apibendrinti taip:

Reikalavimai renkant asmens duomenis

„Atea“ gali tvarkyti (pvz., rinkti, saugoti ir naudoti) asmens duomenis tik tada, kai turi teisėtą verslo interesą, taip pat kai atitinkamas asmuo yra davęs sutikimą arba buvo informuotas, kad jo asmens duomenys yra tvarkomi. Išsami informacija apie šį pranešimą ar sutikimą yra pateikta kitame šio dokumento skyriuje.

Asmenų teisė kontroliuoti savo asmens duomenis

Atsižvelgiant į BDAR įvardintas asmens teises į duomenų privatumą, „Atea“ privalo atsakyti į asmenų, norinčių kontroliuoti savo asmens duomenų naudojimą, užklausas. Pagal BDAR, asmenys turi teisę susipažinti su savo asmens duomenimis, kuriuos turi „Atea“. Asmenys taip pat turi teisę reikalauti, kad asmens duomenys būtų ištaisyti, ištrinti arba apriboti savo asmens duomenų tvarkymą ir naudojimą.

Tvarkymo veiklos dokumentavimas

„Atea“ turi dokumentuoti savo duomenų tvarkymo veiklą, susijusią su asmens duomenimis. Tai apima: kokie asmens duomenys yra tvarkomi, kokių kategorijų duomenų subjektų asmens duomenys yra tvarkomi, kokios techninės ir organizacinės priemonės taikomos apsaugoti asmens duomenis ir sumažinti duomenų saugumo pažeidimo poveikį „Atea“ duomenų tvarkymo veikloje (pvz., pritaikytoji duomenų apsauga).

Duomenų tvarkymo sutartys su klientais/tiekėjais

Kai „Atea“ teikia duomenų tvarkymo paslaugas klientams (pvz., kai „Atea“ prižiūri infrastruktūrą ir sistemas pas klientus ar teikia „Atea“ duomenų centro paslaugas), „Atea“ taip pat turi turėti galiojančią duomenų tvarkymo sutartį su klientu, kuri atitinka BDAR reikalavimus.

Lygiai taip pat, kai „Atea“ tvarko kliento asmens duomenis per subrangovą ar tiekėją (pvz., naudoja programinę įrangą, veikiančią tiekėjo duomenų centre, pvz., debesijos paslaugas), „Atea“ turi turėti galiojančią, BDAR reikalavimus atitinkančią duomenų tvarkymo sutartį su įmone, kuri valdo programinę įrangą/teikia debesijos paslaugą ir tvarko asmens duomenis „Atea“ vardu. Informacija, kuri tvarkoma už ES / EEE ribų, turi būti tvarkoma šalyje arba pagal gaires, kurias valdžios institucijos patvirtino kaip tinkamas duomenų apsaugos priemones (pasirašant „Standart contractual clauses“).

Reikalavimai duomenų saugumo pažeidimo atveju

Asmens duomenų saugumo pažeidimo atveju, dėl kurio gali kilti žalos pavojus asmeniui, „Atea“ privalo pranešti priežiūros institucijai šalyje, kurioje įvyko pažeidimas, per 72 valandas nuo tada, kai sužino apie pažeidimą. Pranešime turi būti aprašytas pažeidimo pobūdis, pateikta duomenų subjektų ir atitinkamų įrašų suvestinė, galimos pažeidimo pasekmės ir priemonės, kurių imamasi.

Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus asmenų teisėms ir laisvėms, nedelsiant turi būti informuojami ir patys asmenys. Gali pakakti viešo paskelbimo, jei atskiras pranešimas nėra galimas.

Pagal Bendrąjį duomenų apsaugos reglamentą, kiekvienos šalies priežiūros institucija gali skirti dideles baudas bendrovei BDAR pažeidimo atveju. Baudos dydis nustatomas pagal pažeidimo pobūdį, žalos duomenų privatumo teisėms mastą ir priemones, kurių ėmėsi bendrovė, kad užkirstų kelią pažeidimui ir jį pašalintų. Didžiausia bauda BDAR pažeidimo atveju yra 4 % metinių bendrųjų pajamų arba 20 milijonų eurų, atsižvelgiant į tai, kuri suma yra didesnė.

Remiantis BDAR reikalavimais, svarbu, kad „Atea“ dokumentuotų visas su asmens duomenimis susijusias veiklas, identifikuotų visas vidines sistemas ir sutartis, susijusias su asmens duomenų tvarkymu. Ši informacija turi būti prieinama kiekvienos šalies vyriausiajam informacijos apsaugos pareigūnui (CISO), kad būtų galima įsitikinti, jog yra taikomos tinkamos priemonės duomenų privatumui apsaugoti. Kiekvienos šalies ir grupės vyriausiojo duomenų apsaugos pareigūno duomenis galite rasti internetiniame puslapyje atea.com/trust.

Pagrindiniai akcentai:

Duomenų privatumas apima asmens kontrolę savo duomenų atžvilgiu, o konkrečiai – gebėjimą nustatyti, kada ir kaip renkami, bendrinami ir naudojami jo duomenys. Asmens duomenys apibrėžiami kaip bet kokia informacija, kurią galima susieti su konkrečiu ir identifikuojamu asmeniu.

„Atea“ taikomi griežti teisiniai reikalavimai tvarkant asmens duomenis, kaip apibrėžta Europos Sąjungos Bendrajame duomenų apsaugos reglamente (BDAR).

Pagal BDAR:

„Atea“ gali tvarkyti (pvz., rinkti, saugoti ir naudoti) asmens duomenis tik tada, kai turi teisėtą verslo interesą, taip pat kai atitinkamas asmuo yra davęs sutikimą arba buvo informuotas, kad jo asmens duomenys yra tvarkomi.

Atsižvelgiant į BDAR įvardintas asmens teises į duomenų privatumą, „Atea“ privalo atsakyti į asmenų, norinčių kontroliuoti savo asmens duomenų naudojimą, užklausas.

„Atea“ turi dokumentuoti savo duomenų tvarkymo veiklos, susijusios su asmens duomenimis, mastą, įskaitant priemones, kurių buvo imtasi siekiant užkirsti kelią duomenų saugumo pažeidimui ir sumažinti jo poveikį. Tam reikia, kad „Atea“ dokumentuotų visas su asmens duomenimis susijusias veiklas, identifikuotų visas vidines sistemas ir sutartis, susijusias su asmens duomenų tvarkymu.

„Atea“ privalo turėti galiojančią duomenų tvarkymo sutartį (DPA) su visais klientais, kuriems ji teikia duomenų tvarkymo paslaugas (pvz., prižiūri infrastruktūrą ir sistemas pas klientą arba savo duomenų centre).

„Atea“ taip pat privalo turėti galiojančią duomenų tvarkymo sutartį (DPA) su subrangovu arba tiekėju, kuris tvarko asmens duomenis „Atea“ vardu (pvz., naudojamasi programine įranga, duomenų saugykla, veikiančia tiekėjo duomenų centre, pvz., debesijos paslaugos).

Asmens duomenų saugumo pažeidimo atveju, dėl kurio gali kilti žalos pavojus asmeniui, „Atea“ privalo pranešti priežiūros institucijai šalyje, kurioje įvyko pažeidimas, per 72 valandas nuo tada, kai sužino apie pažeidimą.

3. „ATEA“ DUOMENŲ APSAUGOS POLITIKA

Rinkdami, tvarkydami ir platindami duomenis „Atea“ darbuotojai visuomet privalo laikytis įmonės duomenų apsaugos politikos. Visi „Atea“ vadovai yra atsakingi už tai, kad verslo procesai jų atsakomybės srityje atitiktų „Atea“ duomenų apsaugos politiką ir kad jų darbuotojai dirbtų pagal šiuos verslo procesus.

Kiekvienas „Atea“ vadovas yra paskirtas duomenų apsaugos administratoriumi, kuris yra atsakingas už konkrečią verslo funkciją savo šalyje ar verslo vienete. Duomenų apsaugos administratoriaus vaidmuo – prižiūrėti, kad visi verslo procesai, priklausantys jo verslo funkcijai, atitiktų „Atea“ duomenų apsaugos politiką. Verslo funkcijos yra: pardavimai / rinkodara, personalas, finansų, konsultavimo paslaugos, techninės priežiūros paslaugos, logistika ir IT.

Duomenų apsaugos administratorius kiekvienai verslo funkcijai yra pavaldus šalies ar verslo vieneto vyriausiajam informacijos apsaugos pareigūnui (CISO). Kiekvienos šalies vyriausiasis informacijos apsaugos pareigūnas (CISO) yra atsakingas už duomenų apsaugos politikos įgyvendinimą toje šalyje ir yra pavaldus grupės vyriausiajam informacijos apsaugos pareigūnui (Group CISO).

Visų pagrindinių Jūsų šalies informacijos apsaugos organizacijos narių kontaktinę informaciją galite rasti „Atea“ internetiniame puslapyje: atea.com/trust. Informacijos saugumo organizavimo santrauka taip pat pateikiama ir šio dokumento priede.

„Atea“ duomenų apsaugos politika apima:

- Informacinių sistemų registravimą;
- Duomenų klasifikavimą;
- Asmens duomenų tvarkymą;
- Klientų susitarimus.

Duomenų apsaugos politikos apžvalga:

Informacinių sistemų registravimas
Prieš „Atea“ darbuotojams pradedant rinkti, tvarkyti ar dalintis informacija, jie turi įsitikinti, kad visos informacinės sistemos, kuriose saugoma ar tvarkoma informacija, yra registruotos ir patvirtintos šalies vyriausiojo informacijos apsaugos pareigūno (CISO). Tai apima ir bet kokias debesijos paslaugas, kurios perkamos ir valdomos ne „Atea“.

Vyriausiasis informacijos apsaugos pareigūnas (CISO), prieš registruodamas sistemą ir tokiu būdu autorizuodamas ją naudojimui „Atea“, atlieka informacinės sistemos IT saugumo ir duomenų privatumo standartų analizę. Analizė yra paremta IT saugumo ir duomenų apsaugos standartų „Atea“ kontroliniu sąrašu ir yra pildoma kartu su „Atea“ grupės vyriausiuoju informacijos apsaugos pareigūnu (Group CISO) bei būsimu sistemos savininku („owner“).

Analizuodamas, ar sistema atitinka „Atea“ informacijos saugumo reikalavimus, vyriausiasis informacijos apsaugos pareigūnas (CISO) taip pat nustato sistemoje saugomų duomenų tipą ir informacijos klasifikavimo žymą. Atlikdamas analizę, vyriausiasis informacijos apsaugos pareigūnas (CISO) taip pat patvirtina politiką, kaip turi būti ištrinti asmens duomenys sistemoje, kai jų nebereikia „Atea“ („Atea“ duomenų mažinimo politika).

Jei informacinė sistema yra valdoma iš išorės ir joje yra asmeninės informacijos, pvz., debesijos pagrindu veikianti personalo valdymo sistema, „Atea“ turi turėti pasirašytą duomenų tvarkymo sutartį (DPA) su paslaugų teikėju, kad būtų laikomasi BDAR. Standartinė DPA, kuri turėtų būti pasirašyta su debesijos paslaugų teikėju, yra „Atea“ informacijos saugos puslapyje intranete: Global Information Security intranet page. Kiekvienos šalies vyriausiasis informacijos apsaugos pareigūnas gali atsakyti į klausimus, susijusius su DPA, kuris taip pat gali dalyvauti DPA pasirašymo su paslaugų teikėjais procese.

„Atea“ darbuotojai negali saugoti arba tvarkyti įmonės duomenų šešėlinėse („Shadow IT“) sistemose, t. y., tose, kurių neregistravo vyriausiasis informacijos apsaugos pareigūnas (CISO). Prieš atliekant reikšmingus duomenų tvarkymo pakeitimus sistemose ar procesuose, „Atea“ darbuotojai privalo informuoti vyriausiąjį informacijos apsaugos pareigūną (CISO), kad jis atliktų naują IT saugumo vertinimą.

Kai sistemą leidžiama naudoti „Atea“, sistemai priskiriamas sistemos savininkas („owner“). Sistemos savininkas yra atsakingas už tai, kad sistema būtų naudojama pagal „Atea“ duomenų apsaugos politiką. Visų pirma, sistemos savininkas privalo užtikrinti, kad prieigos teisės prie informacinės sistemos būtų suteiktos tik tiems darbuotojams, kuriems jų reikia darbo funkcijoms atlikti, ir panaikinamos, kai tik darbo funkcijos pasikeičia ar nutraukiama darbo sutartis ir prieiga tampa nebereikalinga. Pagal duomenų mažinimo politiką, suderintą, kai sistemą buvo leista naudoti, sistemos savininkas taip pat privalo užtikrinti, kad sistemoje saugomi asmens duomenys būtų ištrinti, kai „Atea“ jų nebereikia ar ji neturi teisinio pagrindo juos kaupti.

Duomenų klasifikavimas

Kai sistemą leidžiama naudoti „Atea“, yra fiksuojamas sistemoje saugomų duomenų tipas ir informacijos klasifikavimo žyma, kad būtų užtikrinta tinkama duomenų apsaugos politika.

Tačiau yra daug atvejų, kai „Atea“ darbuotojai tvarko ir dalinasi informacija ne sistemų ribose. Tai apima informaciją, tvarkomą spausdintuose dokumentuose, elektroniniu paštu arba bendrinant elektroninius dokumentus (t. y. Microsoft Word / Excel / PowerPoint failus).

Siekiant užtikrinti, kad ne sistemos priemonėmis tvarkoma informacija būtų valdoma saugiai, „Atea“ darbuotojai privalo suteikti žymą bet kokiam failui, dokumentui ar elektroniniam laiškui atsižvelgiant į jo turinį, kad informacijos gavėjas žinotų, su kokio jautrumo informacija dirba. Šis žymėjimas turi atitikti „Atea“ duomenų klasifikavimo standartus.

„Atea“ duomenų klasifikavimas susideda iš penkių lygių, kurie suskirsto el. laiške arba faile saugomą informaciją nuo mažiausiai jautrios iki jautriausios informacijos. Klasifikavimo priemonės yra integruotos į „Atea“ Microsoft Outlook ir Word/Excel/PowerPoint. „Atea“ darbuotojai gali automatiškai pažymėti el. laišką, dokumentą ar failą teisinga žyma, pasirenkant mygtuką įrankių juostoje.

Yra šie klasifikacijos lygiai:

1. Asmeninė (Non-business): Privatūs elektroniniai susirašinėjimai ir dokumentai, nesusiję su „Atea“.

2. Vieša (Public): Informacija, susijusi su „Atea“, kurią galima platinti viešai.

3. Vidinė (Internal): Informacija, kurią galima platinti „Atea“ viduje arba „Atea“ verslo vienetams ir subrangovams. Neskirta platinti už „Atea“ ribų arba ne sutarties šalims.

4. Konfidencialu (Confidential): Informacija, kuri gavėjo turi būti laikoma privačia ir kuria negali būti dalijamasi be informacijos savininko sutikimo. Tai taikoma ir asmens duomenims, kuriems turi būti taikoma atskira žyma. Žymą „Personal data“ galima pridėti išskleidus pasirinkimą „Confidential“.

5. Griežtai konfidencialu (Strictly confidential): Informacija, kuri gali turėti reikšmingų neigiamų pasekmių „Atea“, jei bus atskleista be leidimo. Turėtų būti saugoma užšifruotu formatu ir negali būti bendrinama be informacijos savininko patvirtinimo. Apima:

- Neskelbtini asmens duomenys: pagal BDAR, tam tikroms asmens duomenų kategorijoms turi būti taikomos papildomos saugumo priemonės. Tai gali būti informacija, susijusi su: etnine kilme, politinėmis pažiūromis, religija, naryste profesinėse sąjungose, genetiniais ar biometriniais duomenimis. Neskelbtini asmens duomenys turėtų būti žymimi kaip „Personal data“, pasirenkant šią žymą iš „Strictly confidential“.
- Neskelbtina verslo informacija: tai – svarbiausia verslo informacija, pvz., pagrindiniai kliento ar tiekėjo duomenys, sutartys ir komercinės sąlygos. Taip pat tai gali būti informacija, kuriai taikomas neatskleidimo arba konfidencialumo susitarimas su klientu arba verslo partneriu. Galiausiai tai gali būti itin neskelbtina intelektinė nuosavybė, pavyzdžiui, verslo koncepcija ir įmonėje sukurta programinė įranga, metodikos ir priemonės.
- Neskelbtina informacija apie kainas: neskelbtina informacija apie kainas yra specifinė konfidencialios informacijos rūšis, kuri gali turėti įtakos „Atea“ akcijų kainai. Apima reikšmingus finansinius duomenis, apie kuriuos dar nebuvo pranešta, arba konfidencialių derybų, susijusių su labai didele sutartimi dėl klientų aptarnavimo arba komercinio susitarimo, statusą.

„Atea“ grupės finansų direktorius (Group CFO) turi būti nedelsiant informuojamas apie visus darbuotojus, turinčius neskelbtinos informacijos apie kainas. Šie darbuotojai registruojami „Atea“ naudojamoje sistemoje „Computershare Insider Management System“ (CIMS). Daugiau informacijos dėl neskelbtinos informacijos apie kainas ir tvarką galima rasti Elgesio kodekse.

Išsamų „Atea“ duomenų klasifikavimo standartų, dokumentų, el. pašto pranešimų žymėjimo bei šifravimo procedūrų aprašymą rasite „Atea“ informacijos saugos intraneto puslapyje: Global Information Security intranet page.

Asmens duomenų tvarkymas

Pagal BDAR, „Atea“ turi teisinius įsipareigojimus tvarkydama asmens duomenis – informaciją, kuri gali būti susijusi su konkrečiu ir identifikuojamu asmeniu. Pagal šiuos teisinius įsipareigojimus, „Atea“ turi dokumentuoti technines ir organizacines priemones, užtikrinančias BDAR reikalavimų laikymąsi. Šis proceso dokumentas turi būti pateiktas valdžios institucijoms, jei jos to paprašo.

Prieš pradedant rinkti asmens duomenis „Atea“, turi būti išsamiai ir tinkamai dokumentuotas verslo procesas, kurio įforminimą peržiūri šalies ar verslo vieneto vyriausiasis informacijos apsaugos pareigūnas (CISO). Kiekvienos verslo funkcijos duomenų apsaugos administratorius yra atsakingas už tai, kad visi asmens duomenų tvarkymo procesai jų funkcijose būtų dokumentuojami ir atnaujinami pagal BDAR.

Dokumentai turi įrodyti, kad „Atea“ ėmėsi pakankamų techninių ir organizacinių priemonių, užtikrinančių asmenų teisių į jų asmens duomenis įgyvendinimą, užkirstų kelią duomenų saugumo pažeidimui ir sumažintų jo poveikį, užtikrintų teisės aktų reikalavimų laikymąsi reaguojant į asmens duomenų pažeidimą. Asmens duomenų rinkimo procesai taip pat turi įtraukti duomenų kiekio mažinimo procedūrą, t. y. asmens duomenų ištrynimą, kai „Atea“ jie tampa nebereikalingi.

Rinkdama asmens duomenis, „Atea“ privalo informuoti asmenį arba gauti jo sutikimą, kad jo asmens duomenys būtų renkami ir naudojami. Pagal BDAR, informavusi arba gavusi asmens sutikimą, „Atea“ turi suteikti šią informaciją:

1. Renkamų ir tvarkomų asmens duomenų kategorijos;
2. Duomenų tvarkymo tikslai ir teisinis pagrindas;
3. Asmens duomenų gavėjai arba gavėjų kategorijos;
4. Laikotarpis, kurį bus tvarkomi asmens duomenys, arba kriterijai, lemiantys šį laikotarpį;
5. Asmens teisės į jų asmens duomenis, įskaitant teisę atšaukti sutikimą ir teisę susipažinti, ištrinti ir ištaisyti asmens duomenis;
6. Asmens teisė pateikti skundą priežiūros institucijai;
7. Jei taikoma, pranešimas, kad duomenys bus tvarkomi ne EU/EEE šalyje, ir patvirtinimas, kad bet koks duomenų tvarkymas atskiroje šalyje bus atliekamas pagal BDAR nuostatas dėl duomenų apsaugos reikalavimų;
8. Jei renkami ypatingi asmens duomenys, „Atea“ turi prašyti ir gauti aiškų sutikimą iš asmens, kurio duomenys yra tvarkomi.

Asmens duomenų privatumo politika yra pateikta „Atea“ informacijos saugos intraneto puslapyje: Global Information Security intranet page.

„Atea“ turi įsipareigojimus pagal BDAR, jei duomenų saugumo pažeidimas yra susijęs su asmens duomenimis. Duomenų pažeidimas – tai informacijos saugumo incidentas, dėl kurio neįgalioti asmenys gauna prieigą prie duomenų arba duomenys neteisėtai ar atsitiktinai prarandami.

Duomenų pažeidimo atveju „Atea“ darbuotojai turi nedelsdami pranešti savo šalies vyriausiajam informacijos apsaugos pareigūnui (CISO). Vyriausiasis informacijos apsaugos pareigūnas (CISO) kartu su „Atea“ grupės informacijos saugumo komanda ištirs duomenų saugumo pažeidimą ir imsis reikiamų veiksmų, kad praneštų apie pažeidimą ir sumažintų bet kokią žalą, padarytą dėl duomenų saugumo pažeidimo.

Jei duomenų saugumo pažeidimas yra susijęs su asmens duomenimis ir sukelia žalos asmeniui pavojų, „Atea“ turi pranešti priežiūros įstaigoms toje šalyje, kurioje buvo padarytas pažeidimas, per 72 valandas po to, kai sužino apie pažeidimą. Pranešime turi būti aprašytas pažeidimo pobūdis, pateikta duomenų subjektų ir atitinkamų įrašų suvestinė, galimos pažeidimo pasekmės ir priemonės, kurių imamasi.

Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus asmenų teisėms ir laisvėms, apie tai turi būti informuojami ir patys asmenys. Gali pakakti viešo paskelbimo, jei atskiras pranešimas nėra galimas.

Klientų susitarimai

„Atea“ prižiūri daugelio klientų infrastruktūrą ir sistemas tiek pas klientą, tiek savo duomenų centre. Tokiais atvejais, „Atea“ pagal sutartį įsipareigoja tvarkyti kliento duomenis ir pagal BDAR turi teisinę prievolę užtikrinti, kad ji tinkamai apsaugos visų asmenų, kurių asmens duomenys yra įtraukti į kliento infrastruktūrą ir sistemas, duomenų privatumo teises.

Siekiant atitikti BDAR reikalavimus, „Atea“ privalo turėti duomenų tvarkymo sutartį (DPA) su klientais, kai „Atea“ tvarko kliento duomenų infrastruktūrą ir sistemas. Duomenų tvarkymo sutartyje turi būti dokumentuotos duomenų tvarkymo veiklos,

kurias „Atea“ atlieka kliento nurodymu, apimtis, pobūdis ir trukmė. Šiame dokumente taip pat turi būti įtraukta santrauka apie tai, kokių tipų ir kokių kategorijų duomenų subjektų asmens duomenis „Atea“ tvarko kliento vardu.

Pagal BDAR reikalavimus, DPA privalo būti ši informacija:

1. „Atea“ tvarko asmens duomenis tik pagal kliento dokumentuotas instrukcijas ir laikosi duomenų apsaugos įstatymų.
2. „Atea“ darbuotojai, kurie tvarko asmens duomenis, įsipareigoja laikytis konfidencialumo. „Atea“ be kliento leidimo nepaskirs subrangovų, kurie tvarkys kliento asmens duomenis.
3. „Atea“ ėmėsi pakankamų techninių ir organizacinių priemonių, kad užtikrintų su klientu suderintą saugumo lygį, atsižvelgiant į tvarkomų duomenų riziką.
4. „Atea“ ėmėsi pakankamų priemonių, kad įvykdytų savo teisinius įsipareigojimus, susijusius su asmenų teisėmis kontroliuoti jų duomenų tvarkymą, kaip aprašyta BDAR.
5. „Atea“ suteiks klientui visą informaciją, būtiną norint įrodyti, kad ji laikosi BDAR nustatytų duomenų privatumo įpareigojimų, ir, jei to prašo klientas, dalyvauja kliento atliekamame atitikties audite.
6. „Atea“ nedelsiant informuos klientą apie bet kokius asmens duomenų pažeidimus.
7. Pasibaigus paslaugų teikimo sutarčiai, „Atea“ ištrins arba grąžins klientui visus asmens duomenis.

Jei „Atea“ naudojasi subrangovais, kad įvykdytų savo duomenų tvarkymo įsipareigojimus klientui (pvz., trečiosios šalies debesijos paslaugos, konsultantai ar infrastruktūros teikėjai), „Atea“ turi turėti atskirą DPA su šiais subrangovais, kur subrangovas pateikia panašius įsipareigojimus, kaip išdėstyta aukščiau.

„Atea“ turi standartines DPA, kurias rekomenduojama naudoti su visais klientais ir subrangovais. DPA galima rasti „Atea“ informacijos saugos intraneto puslapyje: Global Information Security intranet page. Kiekvienos šalies vyriausiasis informacijos apsaugos pareigūnas (CISO) gali atsakyti į klausimus, susijusius su DPA, ir gali padėti parengti DPA su užsakovu ar subrangovu.

Jei asmens duomenų pažeidimas yra susijęs su kliento duomenimis, „Atea“ privalo nedelsiant (kai tik sužino apie duomenų saugumo pažeidimą) pranešti apie tai klientui. „Atea“ turi bendradarbiauti su klientu ir imtis pagrįstų veiksmų, kad užtikrintų, jog klientas galėtų įvykdyti savo įsipareigojimus pranešti apie duomenų saugumo pažeidimą, kaip reikalauja BDAR, ir gali imtis koregavimo ir prevencinių veiksmų, kad sumažintų pažeidimo padarytą žalą.

Pagrindiniai akcentai:

Sistemų registravimas

Visas „Atea“ naudojamas IT sistemas reikia registruoti pas šalies ar verslo vieneto vyriausiąjį informacijos apsaugos pareigūną (CISO). Tai apima ir debesijos paslaugas, kurios valdomos ne „Atea“.

Prieš patvirtindamas, kad sistemą galima naudoti, vyriausiasis informacijos apsaugos pareigūnas (CISO) atliks IT sistemos vertinimą, kad įsitikintų, jog ji atitinka „Atea“ IT saugumo standartus. Užregistravus sistemą, bus paskirtas sistemos savininkas. Sistemos savininko vaidmuo yra užtikrinti, kad sistema būtų naudojama pagal „Atea“ duomenų apsaugos politiką, ypatingą dėmesį skiriant prieigos teisių valdymui.

Duomenų klasifikavimas

Siekiant užtikrinti, kad informacija, tvarkoma ne sistemos priemonėmis, būtų valdoma saugiai, „Atea“ darbuotojai turi suteikti žymas visiems failams, dokumentams ar el. laiškams (atsižvelgiant į turinį), kad informacijos gavėjas žinotų, su kokio jautrumo informacija dirba. Informacijos žymėjimas turi atitikti „Atea“ duomenų klasifikavimo standartus.

Visus asmens duomenų tvarkymo būdus turi dokumentuoti ir peržiūrėti vyriausiasis informacijos apsaugos pareigūnas (CISO). Kiekvienas „Atea“ vadovas yra paskirtas duomenų apsaugos administratoriumi, kuris yra atsakingas už konkrečią verslo funkciją savo šalyje ar verslo vienete. Duomenų apsaugos administratoriaus vaidmuo – prižiūrėti, kad visi verslo procesai, priklausantys jo verslo funkcijai, atitiktų „Atea“ duomenų apsaugos politiką, kaip numatyta BDAR.

Asmens duomenų tvarkymas

Rinkdama asmens duomenis, „Atea“ privalo informuoti asmenį arba gauti jo sutikimą, kad jo asmens duomenys būtų renkami ir naudojami pagal BDAR. BDAR pateikiama daug reikalavimų, susijusių su informavimo turiniu (žr. pagrindinį tekstą).

Duomenų pažeidimas – tai informacijos saugumo incidentas, dėl kurio neįgalioti asmenys gauna prieigą prie duomenų arba duomenys neteisėtai ar atsitiktinai prarandami. „Atea“ turi specialius įsipareigojimus pagal BDAR, jei duomenų saugumo pažeidimas yra susijęs su asmens duomenimis.

Įtarus duomenų saugumo pažeidimą, „Atea“ darbuotojai turi nedelsiant pranešti savo šalies ar verslo vieneto vyriausiajam informacijos apsaugos pareigūnui (CISO). Taip pat gali būti siunčiamas elektroninis laiškas adresu infosec@atea.com, kuris bus perduotas tiesiogiai „Atea“ grupės vyriausiajam informacijos apsaugos pareigūnui (Group CISO).

Pagal BDAR, „Atea“ privalo turėti duomenų tvarkymo sutartį (DPA) su savo klientais, kuriems tvarko duomenų infrastruktūrą ir sistemas. „Atea“ taip pat turi turėti DPA su savo subrangovais ar tiekėjais, kurie tvarko duomenis „Atea“ vardu. BDAR pateikiama daug informacijos reikalavimų, susijusių su DPA turiniu (žr. pagrindinį tekstą).

4. IT INFRASTRUKTŪROS SAUGUMAS: REIKALAUJAMA PRAKTIKA VISIEMS DARBUOTOJAMS

„Atea“ IT infrastruktūrą sudaro visa aparatinė, programinė įranga ir tinklo komponentai, kurių pagalba verslo sistemos ir IT procesai tampa prieinami vartotojams. Duomenų apsauga „Atea“ priklauso nuo visų darbuotojų, kurie atsakingai naudojasi „Atea“ IT infrastruktūros ištekliais.

Žemiau išvardintos taisyklės taikomos visiems „Atea“ darbuotojams, kurie naudojasi „Atea“ IT infrastruktūra, ir apima įrenginių saugumą, prieigą prie sistemų, failų saugojimą, tinklo saugumą, ryšių ir fizinį saugumą. Be to, darbuotojai, atsakingi už „Atea“ IT eksploatavimą, privalo turėti atskirą, išsamesnį mokymą apie IT saugumą, atitinkantį jų pareigas.

Įrenginių sauga:
„Atea“ darbuotojai turi imtis saugos priemonių dirbdami su darbo įrenginiais, pvz., kompiuteriais, planšetiniais kompiuteriais ir išmaniaisiais telefonais. Šie įrenginiai gali būti pavogti, paveikti kenkėjiškų programų ir naudojami asmenų, neturinčių tam teisės. „Atea“ kompiuteriai, planšetiniai kompiuteriai ir išmanieji telefonai visada turi būti stebimi arba laikomi saugioje vietoje. Kai jie nenaudojami, šie prietaisai turi būti užrakinti su PIN arba slaptažodžio apsauga, arba išjungti.

Siekiant užkirsti kelią neteisėtai prieigai prie įrenginyje saugomos informacijos, visi „Atea“ kompiuteriai, planšetiniai kompiuteriai ir išmanieji telefonai turi turėti įdiegtus šifravimo sprendimus. „Atea“ „Windows“ kompiuteriuose naudojamas „Bitlocker“ šifravimo sprendimas, kuris turi būti suaktyvintas prieš naudojimą. „Apple Mac“ modeliuose yra įdiegta funkcija, skirta užšifruoti įrenginyje saugomai informacijai, kuris turi būti suaktyvintas prieš naudojimą. Visuose „iPhone“ ir „iPad“ įrenginiuose yra iš anksto įdiegtas šifravimas. „Android“ mobiliuosiuose ir planšetiniuose kompiuteriuose šifravimas turi būti įjungtas rankiniu būdu. Šifravimas taip pat turėtų būti aktyvuojamas išorinėje atmintyje, pvz., USB diskuose, kuriuos galima lengvai prarasti. Darbuotojai, kuriems reikia pagalbos savo darbo įrenginių šifravimui, gali kreiptis į „Atea“ Servicedesk.

„Atea“ darbuotojams į savo kompiuterius negalima atsisiųsti programinės įrangos, kuri nėra gauta iš „Atea“ IT skyriaus. „Atea“ IT skyrius siūlo daugybę taikomųjų programų per „Accelerator“ portalą: servicemarket.atea.com/accelerator. Šios taikomosios programos yra reguliariai atnaujinamos, kad būtų išlaikytas reikiamas saugos lygis. Jei „Atea“ darbuotojui į savo kompiuterį reikia atsisiųsti išorinę programinę įrangą, kurios nėra „Accelerator“ portale, pirmiausia jis turėtų gauti patvirtinimą iš savo vadovo ir IT departamento savo šalyje.

„Atea“ kompiuteriuose yra iš anksto įdiegtos apsaugos nuo kenkėjiškų programų. Jei turite abejonių dėl apsaugos nuo kenkėjiškų programų, kreipkitės į „Atea“ Servicedesk. Jei antivirusinė programa informuoja apie grėsmę arba jei kompiuteris veikia neįprastai, tai gali būti ženklas, kad Jūsų kompiuteris buvo paveiktas kenkėjiškos programos. Kenkėjiškų programų požymiai kompiuteryje gali būti dažnas vaizdo ekrane „sustingimas“ ar neįprastai lėtas veikimas, taip pat veiksmai, vykstantys be inicijavimo, įskaitant langų atsiradimą ar kitus pasikeitimus ekrane.

Jei įtariate, kad Jūsų kompiuteris buvo paveiktas kenkėjiškos programos, pirmiausia nutraukite darbą kompiuteriu ir išjunkite jį iš tinklo. Tada kreipkitės į „Atea“ Servicedesk ir pateikite informaciją apie tai, kokie simptomai sukėlė įtarimą, kad kompiuteris buvo paveiktas kenkėjiškų programų, ir kokie veiksmai galėjo turėti tam įtakos.

Iš visų darbo įrenginių, kurie bus nebenaudojami, prieš siunčiant juos iš „Atea“ perdirbimui ar pakartotiniam naudojimui reikia ištrinti visus duomenis. Tai turėtų būti daroma laikantis kiekvienoje šalyje taikomų IT procedūrų. Šias procedūras galite rasti savo šalies intraneto tinklalapyje.

Prieiga prie sistemos:
„Atea“ darbuotojams turėtų būti suteikta prieiga prie sistemų tik tada, kai tai reikalinga jų darbo funkcijoms atlikti. Siekiant užtikrinti, kad būtų laikomasi šios politikos, reikia nuolat tikrinti prieigos prie sistemų teises ir užtikrinti, kad prieiga būtų panaikinta, kai tik nebebus reikalinga. Jei „Atea“ darbuotojas turi prieigą prie sistemos, kurios jam nebereikia, jis turėtų nedelsdamas kreiptis į sistemos savininką, kad jis panaikintų prieigos teises.

Kai „Atea“ darbuotojui suteikiamos sistemos prieigos teisės, vartotojo vardas ir laikinas slaptažodis

turi būti pateikiami atskirai. Laikinąjį slaptažodį reikia nedelsiant pakeisti po pirmojo prisijungimo ir jo negalima užsirašyti arba dalintis su kitais. Darbuotojai negali suteikti prieigos teisių kitiems vartotojams. Tai gali atlikti tik sistemos savininkas.

Failų saugojimas:
Visi „Atea“ darbuotojai yra atsakingi už saugų savo darbo failų (pvz., MS Word / Excel / PowerPoint rinkmenų) tvarkymą. Visų tipų failus reikia saugoti „Atea“ vidiniuose bendrinamų failų serveriuose, „Atea“ „OneDrive“ paskyrose arba „Atea“ „SharePoint“ aplinkoje. Jokių kitų išorinių saugojimo svetainių, įskaitant „Dropbox“ ar „Google“ diską, negalima naudoti „Atea“ informacijai saugoti be šalies, kurioje dirbate, IT skyriaus leidimo, nes „Atea“ negali garantuoti šių saugyklų saugumo. „Atea“ darbuotojai neturėtų saugoti įmonės informacijos savo (ne „Atea“) įrenginiuose, nes ši informacija nėra automatiškai šifruojama ir daroma atsarginė duomenų kopija, dėl to kyla duomenų praradimo grėsmė.

Failai turi būti pažymėti pagal „Atea“ duomenų klasifikavimo standartus (5 lygiai). Failai, pažymėti kaip griežtai konfidencialūs, turi būti saugomi užšifruotu formatu. Failai, kuriuose yra asmeninės informacijos, taip pat turi būti atitinkamai pažymėti ir tvarkomi pagal BDAR.

Dėl griežtų BDAR duomenų privatumo reikalavimų, „Atea“ darbuotojai turi būti labai atsargūs saugodami asmens duomenis failuose. Darbuotojai neturėtų naudoti asmens duomenų failuose ne pradiniam tikslui, kuris buvo apibrėžtas ir nurodytas asmeniui, kurio duomenys buvo surinkti. Darbuotojai privalo apriboti dalijimąsi failais, kuriuose yra asmens duomenų, kad būtų užkirstas kelias pažeidimams ar netinkamam šių duomenų naudojimui, ir turi ištrinti asmens duomenis, kai tik jų nereikia. Tai taikoma visiems failams, kuriuos sukūrė „Atea“ darbuotojai, įskaitant MS Word / Excel / PowerPoint failus.

Tinklo saugumas:
„Atea“ domene prijungti galima tik „Atea“ kompiuterius, sukonfigūruotus pagal „Atea“ standartą. „Atea“ mobilieji įrenginiai turi būti jungiami tik prie „Atea“ „WiFi“ tinklo, skirto mobiliesiems įrenginiams. Kiti kompiuteriai ar mobilieji įrenginiai turi būti jungiami prie „Atea“ svečių „WiFi“ tinklo.

„Atea“ siūlo darbuotojams, esantiems ne biure, galimybę prisijungti prie savo vidinio tinklo per „Cisco VPN“ arba „Citrix“. Tai leidžia pasiekti mūsų bendrą failų sistemą, taip pat mūsų bendras verslo sistemas. Jungiantis prie „Cisco VPN“ reikalaujama, kad kompiuteris priklausytų „Atea“, priklausytų „Atea“ domenui (ONE) ir jame būtų įdiegta antivirusinė programinė įranga.

„Atea“ darbuotojams negalima jungtis prie kliento tinklo be išankstinio kliento sutikimo, jei kliento sutartyje nenurodyta kitaip. Su klientu reikia susisiekti kiekvieną kartą, kai „Atea“ darbuotojas prisijungia prie jo tinklo, o „Atea“ darbuotojas visada turi pranešti klientui, kokių veiksmų jis ėmėsi klientų tinkle.

Atea darbuotojai turėtų būti atsargūs, kai kelionės metu naudojasi viešaisiais „WiFi“ tinklais. Duomenų srautas per viešuosius tinklus gali būti stebimas. Prieš naudodamiesi „WiFi“ tinklu, „Atea“ darbuotojai turėtų įsitikinti, kad tinklas yra apsaugotas ir gaunamas iš teisėto paslaugų teikėjo. Jei yra priežasčių abejoti viešojo „WiFi“ tinklo saugumu, „Atea“ darbuotojas turėtų vietoj jo naudoti mobiliojo ryšio tinklą. „Atea“ Servicedesk gali padėti prijungti kompiuterį prie mobiliojo ryšio tinklo.

Tikimasi, kad „Atea“ darbuotojai naudos internetą savo darbinėms funkcijoms atlikti. Naršymas asmeniniais tikslais leidžiamas tik svetainėse, kurių turinys suderinamas su darbo funkcijomis. Internetiniai žaidimai ar azartiniai lošimai draudžiami, o failų bendrinimas ar srautinis medijos transliavimas internetu turėtų apsiriboti su darbu susijusiu turiniu. Visi darbuotojai turėtų žinoti, kad „Atea“ analizuoja interneto srautą, siekiant nustatyti atakas prieš „Atea“, o taip pat gaunama informacija apie netinkamą interneto naudojimą.

Naršant internete būkite atsargūs, įsitikinkite, kad tinklalapis yra tikrai tas, kurio Jums reikia – ypač, jei į jį peradresuojama iš kito puslapio. Niekada nespauskite nuorodų ar langų, esančių tinklalapiuose, kurie atrodo įtartini, nes ten gali būti kenkėjiškų programų, kurios pakenks Jūsų įrenginiui ir įmonės tinklui.

Komunikacija (el. paštas / socialinė žiniasklaida):
El. paštas yra svarbi skaitmeninė „Atea“ darbuotojų komunikacijos priemonė. Tai ir pagrindinis informacijos saugumo pažeidžiamumo šaltinis, nes jis suteikia atakuotojams galimybę nukreipti į „Atea“ kenkėjiškas programas, užsiimti sukčiavimu ir kitomis grėsmėmis patiriant mažas sąnaudas ir su maža baudžiamojo persekiojimo rizika.

Dažnas tapatybės sukčiavimo („phishing“) prieš „Atea“ atvejis yra, kai sukčius tiesiogiai kreipiasi į „Atea“ darbuotoją. El. laiškas atrodo tarsi būtų siųstas iš patikimo šaltinio, dažnai naudojant netikrą tapatybę, pvz., kito „Atea“ darbuotojo,

verslo partnerio ar pardavėjo, pvz., technologijų įmonės ar banko. El. laišku bandoma paveikti „Atea“ darbuotoją, kad jis atliktų laiške nurodytus veiksmus, pvz., pervestų pinigus, įvestų prisijungimo / slaptažodžio duomenis ar kitą slaptą informaciją, arba paspaustų nuorodą ar atidarytų priedą, kuris parsiunčia kenkėjišką programinę įrangą („malware“) į vartotojo kompiuterį ar mobilųjį telefoną.

Laiškas, jo priedas ar nuoroda gali atrodyti nekaltai – pavyzdžiui, bus užmaskuotas kaip kolegos laiškas, tiekėjo pasiūlymas, sąskaita faktūra arba kaip debesijos paskyros, pvz., „OneDrive“, pranešimas. Dėl šios priežasties „Atea“ darbuotojai turi būti labai budrūs tvarkydami el. laiškus ar kitokio pobūdžio pranešimus, net jei jie atrodo gauti iš patikimo šaltinio.

„Atea“ darbuotojai turi neatidaryti nuorodų arba priedų savo prietaisuose, jei jie abejoja elektroninio laiško ar kitokio kontakto su juo teisėtumu. Jei „Atea“ darbuotojas nėra tikras dėl elektroninio laiško teisėtumo arba jei netyčia sureagavo į galimą mėginimą sukčiauti, atidaręs įtartiną nuorodą ar priedą, jis turi nedelsdamas kreiptis į „Atea“ Servicedesk ir pranešti apie šį incidentą.

Darbuotojų el. pašto paskyras dažnai stebi apgavikai, kurie siekia gauti prieigą prie darbuotojo jautrių įmonės duomenų. Dėl šios priežasties el. paštas neturėtų būti naudojamas svarbios verslo informacijos archyviniam saugojimui. Verslo informacija turėtų būti saugoma arba ja dalinamasi saugiomis verslo sistemomis ar failų bendrinimo sprendimais, o ne el. paštu.

Darbinio el. pašto naudojimas asmeniniais tikslais yra leidžiamas, jei naudojimas neprieštarauja „Atea“ verslo interesams arba atliekamas ne darbo valandomis. Asmeniniai susirašinėjimai el. paštu visada turėtų būti suderinami su darbu ir turėtų būti pažymėti kaip „Asmeninė“ (Non-business). Be to, įmonės el. pašto naudojimas asmeniniam bendravimui neturėtų sudaryti įspūdžio, kad laiškas yra „Atea“ paslauga arba įmonės patvirtinimas.

Socialinė žiniasklaida taip pat yra dažnai „Atea“ darbuotojų naudojama bendravimo priemonė. Tinkamai naudojamos socialinės žiniasklaidos priemonės suteikia „Atea“ darbuotojams galimybę įgyti ir perduoti žinias, kurti komercinius santykius ir stiprinti „Atea“ prekės ženklą. Kita vertus, socialinės žiniasklaidos priemonės gali labai pakenkti „Atea“ ir jos darbuotojams, jei jos naudojamos netinkamai, arba jei dalijamasi konfidencialia informacija.

Todėl „Atea“ darbuotojai turėtų būti labai atsargūs, dalydamiesi informacija socialinėje žiniasklaidoje. Bet kokius asmens duomenis (įskaitant vardus, nuotraukas ir kt.) galima bendrinti tik su „Atea“ verslu susijusiuose socialinės žiniasklaidos pranešimuose, jei asmuo, kurio duomenys bus bendrinami, sutinka su jo asmens duomenų naudojimu.

Biuro saugumas:

„Atea“ darbuotojai turėtų nešiotis darbuotojo pažymėjimą. Visi „Atea“ lankytojai turi būti registruojami biuro priimamajame ir turėti lankytojo kortelę matomoje vietoje. Lankytojus reikia pasitikti priimamajame, o po vizito palydėti iki išėjimo, paprašyti grąžinti lankytojo kortelę ir atiduoti ją biuro administratorei. Lankytojų negalima palikti vienų „Atea“ patalpose.

Visa konfidenciali informacija privalo būti pašalinta nuo darbo stalų ir saugiai laikoma, kai ji nenaudojama. Pasibaigus susitikimams, visos rašomosios lentos turi būti nuvalytos. Nereikalingi konfidencialūs dokumentai visada turi būti naikinami dokumentų naikikliais.

Pagrindiniai akcentai:

Įrenginio sauga

Visi „Atea“ kompiuteriai, planšetiniai kompiuteriai ir išmanieji telefonai privalo turėti įdiegtus šifravimo sprendimus, siekiant užkirsti kelią neteisėtai prieigai prie įrenginyje saugomos informacijos. „Atea“ kompiuteriai, planšetiniai kompiuteriai ir išmanieji telefonai visada turi būti stebimi arba laikomi saugioje vietoje. Kai nenaudojami, šie prietaisai turi būti užrakinti su PIN arba slaptažodžio apsauga, arba išjungti.

„Atea“ darbuotojams į savo kompiuterius negalima atsisiųsti programinės įrangos, kuri nėra gauta iš „Atea“ IT skyriaus. Jei „Atea“ darbuotojui į savo kompiuterį reikia atsisiųsti išorinę programinę įrangą, kurios nėra „Atea“, jis pirmiausia turėtų gauti patvirtinimą iš savo vadovo ir IT departamento savo šalyje.

„Atea“ kompiuteriuose yra iš anksto įdiegtos apsaugos nuo kenkėjiškų programų. Jei turite abejonių dėl apsaugos nuo kenkėjiškų programų, kreipkitės į „Atea“ Servicedesk.

Jei įtariate, kad Jūsų kompiuteris buvo užkrėstas kenkėjiškomis programomis arba kitaip paveiktas, pirmiausia nutraukite darbą su kompiuteriu ir atjunkite jį nuo tinklo. Tada kreipkitės į „Atea“ Servicedesk.

Prieiga prie sistemos:

„Atea“ darbuotojams prieiga prie sistemų turi būti suteikta tik tada, kai tai reikalinga jų darbinėms funkcijoms atlikti. Siekiant užtikrinti, kad būtų laikomasi šios politikos, reikia nuolat tikrinti prieigos prie sistemų teises ir užtikrinti, kad prieiga būtų panaikinta, kai tik nebebus reikalinga.

Failų saugojimas

Visi „Atea“ darbuotojai yra atsakingi už saugų savo darbo failų (pvz., MS Word / Excel / PowerPoint rinkmenų) tvarkymą. Failai turi būti pažymėti pagal „Atea“ duomenų klasifikavimo standartus (5 lygiai), atskiras žymas suteikiant failams, kuriuose yra asmens duomenų. Failai, pažymėti kaip griežtai konfidencialūs, turi būti saugomi užšifruotu formatu.

Visų tipų failus reikia saugoti „Atea“ vidiniuose bendrinamų failų serveriuose, „Atea“ „OneDrive“ paskyrose arba „Atea“ „SharePoint“ aplinkoje. Jokių kitų išorinių saugojimo svetainių, įskaitant „Dropbox“ ar „Google“ diską, negalima naudoti „Atea“ failams saugoti be šalies, kurioje dirbate, IT departamento leidimo. „Atea“ darbuotojams nerekomenduojama saugoti įmonės informaciją savo kompiuterio kietajame diske dėl rizikos ją prarasti.

Tinklo saugumas:

„Atea“ domene prijungti galima tik „Atea“ kompiuterius, sukonfigūruotus pagal „Atea“ standartą. „Atea“ mobilieji įrenginiai turi būti jungiami tik prie „Atea“ „WiFi“ tinklo, skirto mobiliesiems įrenginiams. Kiti kompiuteriai ar mobilieji įrenginiai turi būti jungiami prie „Atea“ svečių „WiFi“ tinklo.

„Atea“ darbuotojai turi būti atsargūs naudodamiesi viešaisiais „WiFi“ tinklais. Prieš naudodamiesi „WiFi“ tinklu, „Atea“ darbuotojai turėtų įsitikinti, kad tinklas yra apsaugotas ir gaunamas iš teisėto paslaugų teikėjo.

Prieiga prie interneto naudojant darbo įrenginį turėtų apsiriboti svetainėmis, kurių turinys tinka vykdomoms darbo funkcijoms. Visi darbuotojai turėtų žinoti, kad „Atea“ analizuoja interneto srautą, siekiant nustatyti atakas prieš „Atea“, o taip pat gaunama informacija apie netinkamą interneto naudojimą.

Naršant internete būkite atsargūs, įsitikinkite, kad tinklalapis yra tikrai tas, kurio Jums reikia – ypač, jei į jį peradresuojama iš kito puslapio. Niekada nespauskite nuorodų ar langų, esančių tinklalapiuose, jei jie atrodo įtartini, nes ten gali būti kenkėjiškų programų, kurios pakenks Jūsų įrenginiui ir įmonės tinklui.

Komunikacija (el. paštas / socialinė žiniasklaida):
El. paštas yra svarbi skaitmeninė „Atea“ darbuotojų komunikacijos priemonė. Tai ir pagrindinis informacijos saugumo pažeidžiamumo šaltinis, nes jis suteikia atakuotojams galimybę nukreipti į „Atea“ kenkėjiškas programas, užsiimti sukčiavimu ir kitomis grėsmėmis patiriant mažas sąnaudas ir su maža baudžiamojo persekiojimo rizika.

Dažnas tapatybės sukčiavimo („phishing“) prieš „Atea“ atvejis yra, kai sukčius tiesiogiai kreipiasi į „Atea“ darbuotoją. El. laiškas atrodo tarsi būtų siųstas iš patikimo šaltinio, dažnai naudojant netikrą tapatybę, pvz., kito „Atea“ darbuotojo, verslo partnerio ar pardavėjo, pvz., technologijų įmonės ar banko. El. laišku bandoma paveikti „Atea“ darbuotoją, kad jis atliktų laiške nurodytus veiksmus, pvz., pervestų pinigus, įvestų prisijungimo / slaptažodžio duomenis ar kitą slaptą informaciją, arba paspaustų nuorodą ar atidarytų priedą, kuris parsiunčia kenkėjišką programinę įrangą („malware“) į vartotojo kompiuterį ar mobilųjį telefoną.

„Atea“ darbuotojai turi neatidaryti nuorodų arba priedų savo prietaisuose, jei jie abejoja elektroninio laiško ar kitokio kontakto su juo teisėtumu. Jei „Atea“ darbuotojas nėra tikras dėl elektroninio laiško teisėtumo arba jei netyčia sureagavo į galimą mėginimą sukčiauti, atidaręs įtartiną nuorodą ar priedą, jis turi nedelsdamas kreiptis į „Atea“ Servicedesk ir pranešti apie šį incidentą.

Darbinio el. pašto naudojimas asmeniniais tikslais yra leidžiamas, jei naudojimas neprieštarauja „Atea“ verslo interesams arba atliekamas ne darbo valandomis. Asmeniniai susirašinėjimai el. paštu visada turėtų būti suderinami su darbu ir turėtų būti pažymėti kaip „Asmeninė“ (Non-business).

Atea“ darbuotojai turėtų būti labai atsargūs, dalydamiesi informacija socialinėje žiniasklaidoje. Bet kokius asmens duomenis (įskaitant vardus, nuotraukas ir kt.) galima bendrinti tik su „Atea“ verslu susijusiuose socialinės žiniasklaidos pranešimuose, jei asmuo, kurio duomenys bus bendrinami, sutinka su jo asmens duomenų naudojimu.

Biuro saugumas:
„Atea“ darbuotojai turėtų nešiotis darbuotojo pažymėjimą. Visi „Atea“ lankytojai turi būti registruojami biuro priimamajame ir turėti lankytojo kortelę matomoje vietoje.

Lankytojus reikia pasitikti priimamajame, o po vizito palydėti iki išėjimo, paprašyti grąžinti lankytojo kortelę ir atiduoti ją biuro administratorei. Lankytojų negalima palikti vienų „Atea“ patalpose.

Visa konfidenciali informacija privalo būti pašalinta nuo darbo stalų ir saugiai laikoma, kai ji nenaudojama.

Holdingas
„Atea ASA“
„Atea ASA“
Brynsalleen 2
Box 6472 Etterstad
NO-0605 Oslas
+47 22 09 50 00
Org. No. 920 237 126
investor@atea.com
atea.com

Norvegija
„Atea AS“
Brynsalleen 2
Box 6472 Etterstad
NO-0605 Oslas
+47 22 09 50 00
Org. No. 976.239.997
info@atea.no
atea.no

Švedija
„Atea AB“
Kronborgsgränd 1
Box 18
SE-164 93 Kista
+46 (0)8 477 47 00
Org. No. 556448-0282
info@atea.se
atea.se

Danija
„Atea“ A/S
Lautrupvang 6
DK-2750 Ballerup
+45 70 25 25 50
Org. No. 25511484
info@atea.dk
atea.dk

Suomija
Atea Oy
Jaakonkatu 2
PL 39
FI-01621 Vantaa
+ 358 (0)10 613 611
Org. No. 091 9156-0
customercare@atea.fi
atea.fi

Lietuva
UAB „Atea Baltic“
J. Rutkausko 6
LT-05132 Vilnius
+370 5 239 7899
Org. No. 300125003
info@atea.lt
atea.lt

Grupės logistika
„Atea“ Logistics AB
Smedjegatan 12
Box 159
SE-351 04 Växjö
+46 (0)470 77 16 00
Org. No. 556354-4690
customer.care@atea.se

Bendrosios grupės paslaugos
„Atea Global Services“ SIA
Mukusalas 15
LV-1004 Ryga
+371 67359600
Org. No. 50203101431
rigainfo@atea.com
ateaglobal.com

ATEA