TP2B THE PLACE TO BE

ATEA

INFORMĀCIJAS SISTĒMU DROŠĪBAS RISKA PĀRVALDĪBA: POLITIKA DARBINIEKIEM

1.0. redakcija – publicēts 2019.

VADĪTĀJA VĒSTULE

Mūsu, Atea, misija ir "Veidot nākotni ar IT".

Mēs ticam, ka informāciju tehnoloģijas savienojumā ar zināšanām un radošumu var uzlabot visas sabiedrības produktivitāti un dzīves līmeni. Mēs atbalstām uzņēmumus un valsts sektora organizācijas digitālo risinājumu radīšanā, kas ļauj tiem sasniegt vairāk ar lielāku efektivitāti un mazāku resursu patēriņu.

Tajā pašā laikā mēs apzināmies tehnoloģijām raksturīgos riskus saistībā ar aizvien lielāka apjoma informāciju glabāšanu un apstrādi. Tā kā uzņēmumi apstrādā aizvien vairāk datu un automatizē procesus caur to IT sistēmām un tīkliem, uzņēmumi saskaras ar arvien lielākiem draudiem saistībā ar datu zādzībām, identitātes viltošanām un kiberuzbrukumu izraisītiem darbības traucējumiem. Datu aizsardzības pārkāpuma rezultātā iespējams piekļūt personas datiem bez personas piekrišanas un izmantot tos ļaunprātīgi, lai kaitētu šai personai un pārkāptu personas tiesības uz privātumu.

Atea ir vadošais informācijas tehnoloģiju pakalpojumu piegādātājs Ziemeļvalstu un Baltijas reģionos ar īpašu atbildību nodrošināt, lai tā darbība atbilstu stingriem informācijas sistēmu drošības standartiem. Atea izstrādā, ievieš un nodrošina IT infrastruktūru risinājumus lielākajām un ietekmīgākajām organizācijām mūsu reģionos. Lielākie pārdošanas apjomi tiek nodrošināti valsts un pašvaldību iestādēm, tostarp īpaši sensitīvu datu apstrādātājiem, piemēram, armijai un policijai. Mēs piedāvājam arī ļoti būtiskus IT risinājumus mūsu reģionu lielāko korporāciju darbības nodrošināšanai.

Šis dokuments ir rokasgrāmata informācijas sistēmu drošības risku pārvaldībai Atea uzņēmumā. Tajā ir atspoguļots galveno drošības risku, datu aizsardzības politiku un pārvaldības procedūru pārskats, kas skar ikvienu mūsu uzņēmumā. Darbiniekiem, kuriem ir īpaši pienākumi IT darbībās un sistēmu administrēšanā, būs atsevišķa, plašāka pārbaude par informācijas sistēmu drošību un datu aizsardzības politiku, jo viņu amats to pieprasa.

Dokuments ir sadalīts četrās nodaļās, katras nodaļas beigās ir tās kopsavilkums ar būtiskākajiem faktiem. Visās četrās nodaļās ir detalizēti aprakstīta informācija, jo tas ir sarežģīts un kritiski svarīgs jautājums. Svarīgi, lai darbinieki atcerētos katras nodaļas beigās izceltos būtiskākos faktus un, ja nepieciešams, spētu atsaukties uz pārējo dokumenta nodaļu.

Šā dokumenta saturs ir jāpārzina visiem Atea darbiniekiem. Lai pārliecinātos, ka visi Atea darbinieki ir sapratuši šā dokumenta saturu, Rīcības kodeksa pārbaudē ir iekļauti desmit ar informācijas sistēmu drošību saistīti jautājumi. Pārbaude ir obligāta visiem Atea darbiniekiem. Lai apgūtu Atea informācijas sistēmu drošības politiku un sagatavotos Rīcības kodeksa pārbaudei, darbiniekiem ir pieejams tiešsaistes apmācības kurss.

Atea ir liela organizācija ar teju 90 birojiem septiņās valstīs. Grupā un katrā valstī ir norīkots informāciju sistēmu drošības pārvaldnieks, kas atbalstīs informācijas sistēmu drošības politikas ieviešanu visā Atea organizācijā.

Steinars Senstebijs
(*Steinar Sønsteby)*
Ģenerāldirektors

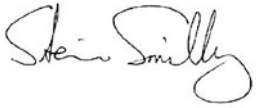
Ja jums ir jautājumi saistībā ar informācijas sistēmu drošību Atea, lūdzam tos izklāstīt pēc būtības:

- Ja jums ir bažas, ka jūsu dators var būt inficēts ar ļaunprogrammatūru, vai ir vispārīgi jautājumi par IT drošību, lūdzam sazināties ar Atea Servicedesk
- Lai ziņotu par aizdomīgiem e-pasta ziņojumiem, krāpniecības mēģinājumiem vai jebkura cita veida gadījumiem, kas varētu radīt draudus Atea informācijas sistēmu drošībai, lūdzam sazināties ar Atea Servicedesk
- Lai ziņotu par aizdomām par personas datu vai uzņēmuma datu aizsardzības pārkāpumiem informācijas sistēmās un dokumentos (neatļautu izpaušanu), lūdzam sazināties ar savas attiecīgās valsts informācijas sistēmu drošības pārvaldnieku. Iespējams arī nosūtīt e-pasta ziņojumu uz infosec@atea.com.

Ja vēlaties sazināties tieši ar Atea grupas, jūsu valsts vai kopīga pakalpojuma vienības informācijas sistēmu drošības pārvaldnieku (ISDP), viņu vārdi ir atrodami Atea atbilstības tīmekļa vietnē: atea.com/trust. Ikviens e-pasta ziņojums, kas nosūtīts uz infosec@atea.com tiks tieši novirzīts Atea grupas informācijas sistēmu drošības pārvaldniekam.

Mēs priecāsimies saņemt jūsu jautājumus un viedokli, un apsolām, ka netiks veiktas nekādas represijas par jebkurām izteiktām bažām vai viedokli. Tomēr, ja vēlaties ziņot anonīmi, varat arī iesniegt ziņojumu, izmantojot trauksmes cēlēju uzticības tālruni. Saiti uz trauksmes cēlēju uzticības dienesta kontaktinformāciju iespējams atrast Atea atbilstības tīmekļa vietnē: atea.com/trust. Bažas, par kurām ir ziņots trauksmes cēlēju uzticības dienestam, tiek nosūtītas neatkarīgam juristu uzņēmumam, kuri veic problēmas kopsavilkumu un ziņo par to Atea organizācijai attiecīgajā līmenī.

Stingru informācijas sistēmu drošības standartu uzturēšana ir būtiska Atea uzņēmējdarbībai, kā arī mūsu spējai strādāt ar klientiem un partneriem, lai risinātu vissvarīgākos IT izaicinājumus mūsu reģionā. Pateicamies par Atea informācijas sistēmu drošības politikas ievērošanu un Atea veidošanu par "labu vietu, kur strādāt".



Būtiskākie fakti:

Atea ir būtiski, lai visi darbinieki uzturētu stingrus informācijas sistēmu drošības standartus.

Grupā un katrā valstī ir norīkots informāciju sistēmu drošības pārvaldnieks, lai atbalstītu informācijas sistēmu drošības politikas ieviešanu visā Atea organizācijā. Informācijas sistēmu drošības pārvaldnieku saraksts ir redzams Atea atbilstības tīmekļa vietnē: atea.com/trust.

Ja jums ir jautājumi vai bažas saistībā ar informācijas sistēmu drošību Atea, lūdzam tos izklāstīt pēc būtības:

- Ja jums ir bažas, ka jūsu dators var būt inficēts ar ļaunprogrammatūru, vai ir vispārīgi jautājumi par IT drošību, lūdzam sazināties ar Atea Servicedesk
- Lai ziņotu par aizdomīgiem e-pasta ziņojumiem, krāpniecības mēģinājumiem vai jebkura cita veida gadījumiem, kas varētu radīt draudus Atea informācijas sistēmu drošībai, lūdzam sazināties ar Atea Servicedesk
- Lai ziņotu par aizdomām par personas datu vai uzņēmuma datu aizsardzības pārkāpumiem informācijas sistēmās un dokumentos (neatļautu izpaušanu), lūdzam sazināties ar savas attiecīgās valsts informācijas sistēmu drošības pārvaldnieku.
- Iespējams arī nosūtīt e-pasta ziņojumu uz infosec@atea.com, kas tiks tieši novirzīts Atea grupas informācijas sistēmu drošības pārvaldniekam.

Saturs

1. INFORMĀCIJAS SISTĒMU DROŠĪBA - PĀRSKATS UN RISKA PĀRVALDĪBA

Informācija ir svarīga jebkuras organizācijas darbībai. Informācijas sistēmu drošības pārvaldība (ISDP) ir politiku, procedūru, rīku un darbību kopums, kuru lieto organizācija, lai aizsargātu savus informācijas aktīvus no nepilnvarotas piekļuves un ļaunprātīgas izmantošanas.

Lai izstrādātu ISDP, ir nepieciešams, lai organizācija identificē tai piederošos informācijas aktīvus. Tie iekļauj visus datus, kurus apstrādā organizācija, neskatoties uz to formu: digitālu, papīra vai mutisku. Atea šī informācija var būt iekšējai lietošanai vai tie var būt ārēji dati, kurus Atea pārvalda un apstrādā, tādējādi sniedzot pakalpojumu saviem klientiem.

Informācijas sistēmu drošības pārvaldības mērķis ir aizsargāt un saglabāt informācijas aktīvu konfidencialitāti, integritāti un pieejamību.

- **Konfidencialitāte** nozīmē, ka informācija ir pieejama tikai pilnvarotām personām.
- **Integritāte** nozīmē, ka informācija tiek glabāta tādā veidā, ka tā ir pilnīga un precīza.
- **Pieejamība** nozīmē, ka pilnvaroti lietotāji var piekļūt datiem un izmantot tos, kad tas ir nepieciešams.

Lai šos mērķus sasniegtu, organizācijai vajadzētu veikt riska novērtēšanu, lai noteiktu, kā tās informācijas aktīvi ir pakļauti potenciāliem informācijas drošības draudiem. Pēc tam tā var izveidot informācijas sistēmu drošības pārvaldības sistēmu, kas bez liekām izmaksām vai produktivitātes krišanās var efektīvi pārvaldīt un kontrolēt šos riskus.

Risku novērtējums Atea

Atea biznesam ar augstāko prioritāti ir identificēti šādi informācijas drošības riski:

1. **Fiziski zaudējumi:**
   Informācijas aktīvi tiek glabāti fiziskās ierīcēs, kuras var pazaudēt, nozagt vai sabojāt. Piekļuves kontrole, šifrēšana un datu dublēšana ir būtiska, lai ierobežotu fizisko aktīvu iespējamos riskus, piemēram, datoriem, mobilajiem tālruņiem, serveriem un noliktavai. Datu centri ir īpaši neaizsargāti, un tie ir jāaizsargā no vides apdraudējumiem, tostarp pārāk augstas vai zemas temperatūras un uguns.

2. **Identitātes viltošana:**
   Atea pastāvīgi tiek pakļauta krāpšanas mēģinājumiem no krāpnieku puses, kuri izmanto viltus identitātes vai maldināšanu, lai izmantotu darbinieka uzticību. Parasti krāpniecības mēģinājumu mērķis ir apzagt Atea vai iegūt neautorizētu pieeju Atea sistēmām un tīkliem.

   Viens no identitātes viltošanas veidiem, kas ir mēģināts pret Atea, ir viltotu vai zagtu klientu datu izmantošana nolūkā pasūtīt IT aprīkojumu no Atea interneta veikala. Lai samazinātu krāpniecisku darījumu risku, papildus interneta veikala piekļuves kontrolei Atea ir izstrādāta kārtība, lai pārbaudītu jaunus klientu kontus un noteiktu neparastu darbību esošo klientu kontos.

   Vēl viens identitātes viltošanas (pikšķerēšanas) veids ir krāpnieku tieša sazināšanās ar Atea darbiniekiem, visbiežāk izmantojot e-pasta ziņojumus. Šis e-pasta ziņojums ir no šķietami uzticama avota, bieži vien izmantojot viltus identitāti, piemēram, cita Atea darbinieka, biznesa partnera vai pakalpojumu sniedzēja (tehnoloģiju uzņēmuma vai bankas). E-pasta ziņojuma mērķis ir panākt Atea darbinieka atbildes darbību, piemēram, naudas pārskaitīšanu, pieteikšanās/paroles vai sensitīvu datu ievadīšanu vai klikšķināšanu uz saites vai pielikuma, kurš lietotāja datorā vai mobilajā telefonā lejupielādē ļaunprogrammatūru.

   E-pasts, pielikums vai saite ir šķietami nekaitīgi - piemēram, tie ir maskēti kā vēstule no kolēģa, piedāvājums/rēķins no pārdevēja vai kā paziņojums no mākoņpakalpojuma konta, piemēram, OneDrive. Šā iemesla dēļ Atea darbiniekiem ir jābūt ļoti uzmanīgiem un jāizvērtē jebkurš e-pasts vai cita veida saziņa pret krāpšanas iespējamību, pat ja paziņojums šķiet no uzticama avota.

   Atea darbiniekiem nekad nevajadzētu atvērt saites vai pielikumus, izmantojot savas ierīces, ja viņiem ir šaubas par e-pasta vai komunikācijas leģitimitāti. Ja Atea darbinieks nav pārliecināts par e-pasta leģitimitāti vai, ja darbinieks

nejauši ir reaģējis uz iespējamu krāpšanas mēģinājumu,atverotaizdomīgusaitivaipielikumu, viņa pienākums ir nekavējoties sazināties ar Atea Servicedesk un ziņot par iespējamu apdraudējumu.

Kaut arī e-pasta ziņojuma nosūtīšana ir vispopulārākā ar darbu saistītā pikšķerēšanas uzbrukuma metode, Atea darbiniekiem ir jāuzmanās arī no citiem krāpnieciskas komunikācijas veidiem, tajā skaitā telefoniskiem pieprasījumiem vai ielūgumiem sociālo mediju platformās.

3. Uzņēmumu noslēpumu zādzība:

Ja neautorizētas personas iegūst piekļuvi Atea informācijas sistēmām, viņi var mēģināt nozagt konfidenciālu informāciju, kas ir Atea biznesa sensitīvā informācija. Tā var ietvert konfidenciālu biznesa informāciju, piemēram, klienta vai piegādātāja datus, līgumus un komerciālus noteikumus. Tā var ietvert arī intelektuālo īpašumu, piemēram, uzņēmējdarbības koncepcijas, produktu vai pakalpojumu dizainu un iekšēji izstrādātu programmatūru, metodoloģijas un rīkus.

Arī darbinieki ar piekļuvi galvenajām sistēmām var mēģināt nozagt Atea komercnoslēpumus īpaši tādā gadījumā, ja viņi plāno pamest uzņēmumu. Lai samazinātu risku, piekļuve informācijai ir jāpiešķir tikai tiem darbiniekiem, kuriem informācija ir nepieciešama pienākumu pildīšanai. Piekļuve sistēmai būtu pastāvīgi jāpārbauda, lai nodrošinātu, ka šis princips tiek saglabāts un ka lietotāja piekļuves tiesības tiek pārtrauktas, kad tās vairs nav nepieciešamas.

Papildus piekļuves kontrolei Atea izmanto informācijas drošības un notikumu pārvaldības (SIEM) rīkus, lai analizētu žurnāla informāciju un to, kādas darbības ir veiktas tā sistēmās.

4. Uzņēmējdarbības pārtraukšana:

Atea uzņēmējdarbība ir atkarīga no tā IT sistēmām. Ja ir noticis piekļuves kontroles pārkāpums vai sistēmas tiek ļaunprātīgi izmantotas, var tikt nopludināta darbinieku vai biznesa partneru privātā informācija. Informācija, kas ir svarīga Atea uzņēmējdarbībai, var tikt bojāta vai izdzēsta. Visbeidzot, Atea pārvaldības sistēmas uzlaušanas gadījumā neautorizētas personas var ievadīt vai apstiprināt biznesa darījumus. Visi šie notikumi ir nopietns traucējums Atea uzņēmējdarbībai.

Pastāv arī risks, ka Atea darbības tiks traucētas, izmantojot izsmalcinātu sistēmas uzlaušanu, kas izslēdz galvenās IT sistēmas vai tīklus. Sistēmas var tikt inficētas ar ļaunprogrammatūru, kas neļauj lietotājiem piekļūt svarīgām funkcijām vai nolasīt datnes, kamēr nav samaksāta izpirkuma maksa („izspiedējprogrammatūra"). Tīkli vai serveri var tikt pārpludināti ar datu plūsmu vai pieprasījumiem, lai tie vairs nespētu apstrādāt likumīgus darījumus („pakalpojumatteices uzbrukums"). Šo uzbrukumu mērķis var būt Atea vai tā klienti, kuru datus Atea pārvalda no sava datu centra.

5. Kaitējums līgumsaistībām:

Atea ir noslēgti konfidencialitātes līgumi ar daudziem klientiem, pārdevējiem un biznesa partneriem. Atea ir noslēgti arī pakalpojumu sniegšanas līgumi un datu apstrādes līgumi ar klientiem, kuri izmanto Atea IT pakalpojumus un atbalstu.

Atea IT drošības pārkāpuma dēļ var gadīties, ka Atea pārkāpj ar klientiem un citiem biznesa partneriem noslēgtos konfidencialitātes, pakalpojumu sniegšanas un datu apstrādes līgumus. Tā rezultātā pret Atea var tikt uzsāktas tiesvedības par zaudējumu atlīdzināšanu saistībā ar līguma nosacījumu pārkāpšanu. Papildus tiešajiem zaudējumiem IT drošības pārkāpums var izraisīt ilgstošu kaitējumu Atea biznesa attiecībām ar tā klientiem un partneriem.

Pat gadījumos, kad Atea nav noslēgts sadarbības līgums, pret Atea var būt juridiskas prasības no uzņēmumiem vai privātpersonām, ja viņu dati tiek nozagti vai ļaunprātīgi izmantoti un Atea nav pievērsis nepieciešamo uzmanību, apstrādājot to datus.

6. Reglamentējošie sodi:

Ņemot vērā to, ka Atea ir iekļauts Oslo biržas sarakstā, tā pienākums ir ievērot stingras juridiskās prasības, apstrādājot datus, kas nav zināmi tirgū un kuriem var būt ietekme uz tā akciju cenu („cenu jutīga informācija"). Tas var ietvert informāciju par veiksmīgiem, jauniem

līgumiem vai finanšu rezultātiem, par kuriem vēl nav ziņots sabiedrībai.

Atea ir konfidenciāli jāpārvalda cenu ziņā jutīga informācija, lai nodrošinātu, ka šī informācija netiek izplatīta ārpus ierobežota skaita reģistrētu uzņēmuma darbinieku, kuriem piekļuve ir piešķirta tiešo pienākumu veikšanai. Uzņēmumam ir jāreģistrē darbinieki, kuriem ir piešķirta piekļuve cenu ziņā jutīgai informācijai, un uz tiem attiecas īpašas konfidencialitātes prasības un Atea akciju tirdzniecības ierobežojumi. Saskaņā ar Norvēģijas Vērtspapīru tirdzniecības likumu šo juridisko prasību pārkāpšanas gadījumā var tikt uzsākta kriminālvajāšana un piešķirti regulējoši sodi.

Personasdatuaizsardzībaspārkāpumagadījumā Atea var tikt piešķirtas sankcijas saskaņā ar Eiropas Savienības Vispārējo datu aizsardzības regulu (GDPR) . Tā kā GDPR prasības ir diezgan plašas, šī tēma tiks aplūkota atsevišķi šā dokumenta nākamajā nodaļā par datu privātumu.

Būtiskākie fakti:

Visiem darbiniekiem jābūt ļoti uzmanīgiem, strādājot ar informācijas un IT sistēmām, lai novērstu drošības pārkāpumus.

IT aprīkojums var tikt nozaudēts, nozagts vai sabojāts. Tāpēc, lai ierobežotu iespējamos informācijas sistēmu drošības riskus, ir svarīga piekļuves kontrole, šifrēšana un datu dublēšana.

Atea pastāvīgi tiek pakļauta krāpšanas mēģinājumiem no krāpnieku puses, kuri izmanto viltus identitātes vai maldināšanu, lai izmantotu darbinieka uzticību. Ņemiet vērā, ka jebkurš e-pasts vai cita veida ziņojums, ko saņemat, var būt krāpšanas mēģinājums, pat ja šķiet, ka tas ir no likumīga avota (ieskaitot e-pastu vai ziņojumu no Atea darbinieka, klienta, tehnoloģiju pārdevēja vai sociālo tīklu konta).

Esiet uzmanīgi saistībā ar jebkādu neparastu saziņu vai darbību, ko jūs ievērojat. Ja jums ir aizdomas, ka jūs esat krāpniecības mērķis, izmantojot e-pastu vai citu saziņas veidu, lūdzu, sazinieties ar Atea Servicedesk. Nereaģējiet uz jebkādu aizdomīgu saziņu, piemēram, atverot e-pasta pielikumus un ārējās saites, vai apstrādājot pasūtījumus un maksājumus.

Lai samazinātu informācijas zādzības vai ļaunprātīgas izmantošanas risku, darba ņēmējiem piekļuve informācijai ir jāpiešķir tikai pēc nepieciešamības. Piekļuve sistēmai būtu pastāvīgi jāpārbauda, lai nodrošinātu, ka lietotāja piekļuves tiesības tiek pārtrauktas, kad tās vairs nav nepieciešamas.

Informācijas sistēmas drošības pārkāpums var nopietni kaitēt Atea, traucējot tā uzņēmējdarbību, liekot Atea pārkāpt līgumsaistības ar klientiem un biznesa partneriem, izraisot regulējošu sodu piešķiršanu un kaitējot Atea reputācijai un biznesa attiecībām.

2. DATU PRIVĀTUMS - PĀRSKATS UN RISKA PĀRVALDĪBA

Datu privātums nozīmē personas kontroli pār saviem datiem, konkrēti, spēju noteikt, kad un kā viņa/-as dati ir apkopoti, koplietoti un izmantoti. Personas dati tiek definēti kā jebkāda veida informācija, kas var būt saistīta ar konkrētu un identificējamu personu.

Datu privātums ir atkarīgs no informācijas sistēmu drošības, t.i., kā dati tiek aizsargāti pret nesankcionētu piekļuvi un ļaunprātīgu izmantošanu. Tomēr datu privātums ir arī kas vairāk par informācijas sistēmu drošību, tas iekļauj arī indivīda tiesību aizsardzību uz saviem datiem. Precīzāk - kā organizācija nodrošina iespēju katrai personai kontrolēt savu personas datu izmantošanu mirklī, kad organizācija apkopo un apstrādā informāciju par šo personu.

Mēs, Atea, uzskatām, ka datu privātums ir cilvēka pamattiesības, un mēs esam apņēmušies apstrādāt personas datus tādā veidā, kas pilnībā ievēro šīs tiesības. Atea pienākums ir ievērot stingras juridiskās prasības, apstrādājot personas datus saskaņā ar Eiropas Savienības Vispārējo datu aizsardzības regulu (GDPR).

Kā GDPR prasības attiecas uz Atea:

Prasības personas datu apkopošanā
Atea ir tiesības apstrādāt (piemēram, apkopot, uzglabāt un izmantot) personas datus tikai likumīgas uzņēmējdarbības intereses gadījumā, un ja attiecīgā persona ir devusi piekrišanu vai ir informēta par to, ka tiek apstrādāti viņa/-as personas dati. Informācija par šo paziņojumu vai piekrišanu ir aprakstīta šā dokumenta nākamajā nodaļā.

Personu tiesības kontrolēt savus personas datus
Ievērojot GDPR noteikumus, Atea pienākums ir respektēt personas pieprasījumu kontrolēt savu personas datu izmantošanu saskaņā ar viņa/-as tiesībām uz datu privātumu. Saskaņā ar GDPR indivīdiem ir tiesības piekļūt saviem personas datiem, kuru turētājs ir Atea. Indivīdiem ir arī tiesības labot kļūdas savos personas datos, dzēst tos vai ierobežot to apstrādi un izmantošanu.

Apstrādes darbību dokumentācija
Atea pienākums ir dokumentēt datu apstrādes darbības apjomu attiecībā uz personas datiem. Tajā ir jāiekļauj apraksts par to, kāda veida personas dati tiek apstrādāti un kādām personu kategorijām. Tajā jāiekļauj arī apraksts par to, kādi tehniskie un organizatoriskie pasākumi ir veikti, lai novērstu un mazinātu datu aizsardzības pārkāpuma ietekmi Atea datu apstrādes darbībās („integrēta privātuma aizsardzība").

Datu apstrādes līgumi ar klientiem / pārdevējiem
Kad Atea saviem klientiem sniedz datu apstrādes pakalpojumus (piemēram, kad Atea klientu vietā pārvalda datu infrastruktūru un lietojumprogrammas, esot pie klienta, vai no saviem datu centriem), Atea ir jābūt ar klientu arī noslēgtam datu apstrādes līgumam, kas atbilst GDPR prasībām.

Tāpat, kad Atea apstrādā personas datus ar apakšuzņēmēja vai pārdevēja starpniecību (piemēram, ja tas lieto programmatūras, kas darbojas pārdevēja datu centrā, piemēram, mākoņpakalpojumi), Atea ir jābūt spēkā esošam, GDPR atbilstošam datu apstrādes līgumam ar uzņēmumu, kas Atea vārdā pārvalda lietojumprogrammu un apstrādā personas datus. Informācijai, kas tiek apstrādāta ārpus ES/EEZ, jāatrodas valstī vai sistēmā, ko valsts iestādes ir apstiprinājušas kā piemērotas datu aizsardzības pasākumiem.

Prasības datu aizsardzības pārkāpuma gadījumā
Datu aizsardzības pārkāpuma gadījumā, kura rezultātā var tikt veikts kaitējums indivīdam, Atea pienākums ir 72 stundu laikā pēc tam, kad tas ir uzzinājis par pārkāpumu, ziņot tās valsts uzraudzības iestādei, kurā pārkāpums noticis. Paziņojumā jāapraksta pārkāpuma veids, skarto datu subjektu un attiecīgo dokumentu kopsavilkums, pārkāpuma iespējamās sekas un veiktie pretpasākumi.

Ja personai, kuru personas datu aizsardzība ir pārkāpta, pastāv liels kaitējuma risks, viņš/-a ir nekavējoties jāinformē par pārkāpumu. Ja individuāls paziņojums nav iespējams, ir pietiekams publisks paziņojums.

Saskaņā ar GDPR katras valsts uzraudzības iestāde GDPR pārkāpuma gadījumā var uzlikt uzņēmumam augstus sodus. Sodu apmērs ir balstīts uz pārkāpuma raksturu, datu privātuma tiesību pārkāpuma apmēru un pasākumiem, ko uzņēmums ir veicis, lai novērstu un apturētu pārkāpumu. Maksimālais sods GDPR pārkāpuma gadījumā ir 4% no uzņēmuma gada ienākumiem pasaulē vai 20 miljoni eiro, atkarībā no tā, kurš ir lielāks.

Pamatojoties uz GDPR prasībām, ir ļoti svarīgi, ka Atea dokumentē visas ikdienišķās darbības, kas saistītas ar personas datiem, un identificē visus iekšējos pielietojumus un līgumus, kas saistīti ar personas datu apstrādi. Lai pārliecinātos, ka ir ieviesti atbilstoši pasākumi datu privātuma aizsardzībai, ir jābūt iespējai iegūt informāciju pie katras valsts informācijas sistēmu drošības pārvaldnieka. Katras valsts un grupas informācijas sistēmu drošības pārvaldnieka kontaktinformāciju iespējams iegūt Atea atbilstības tīmekļa vietnē.

Būtiskākie fakti:

Datu privātums nozīmē personas kontroli pār saviem datiem, konkrēti, spēju noteikt, kad un kā viņa/-as dati ir apkopoti, koplietoti un izmantoti. Personas dati tiek definēti kā jebkāda veida informācija, kas var būt saistīta ar konkrētu un identificējamu personu.

Atea pienākums ir ievērot stingras juridiskās prasības, apstrādājot personas datus saskaņā ar Eiropas Savienības Vispārējo datu aizsardzības regulu (GDPR).

Saskaņā ar GDPR:

Atea ir tiesības apstrādāt (piemēram, apkopot, uzglabāt un izmantot) personas datus tikai likumīgas uzņēmējdarbības intereses gadījumā, un ja attiecīgā persona ir devusi piekrišanu vai ir informēta par to, ka tiek apstrādāti viņa/-as personas dati.

Ievērojot GDPR noteikumus, Atea pienākums ir respektēt personas pieprasījumu kontrolēt savu personas datu izmantošanu saskaņā ar viņa/-as tiesībām uz datu privātumu.

Atea pienākums ir dokumentēt datu apstrādes darbību apjomu attiecībā uz personas datiem, tostarp par to, kādi pasākumi veikti, lai novērstu un samazinātu datu aizsardzības pārkāpuma ietekmi. Lai to izpildītu, Atea ir jādokumentē visas ikdienišķās darbības, kas saistītas ar personas datiem, un jāidentificē visus iekšējos pielietojumus un līgumus, kas saistīti ar personas datu apstrādi.

Atea rīcībā ir jābūt spēkā esošam datu apstrādes līgumam ar visiem klientiem, kuriem tas sniedz datu apstrādes pakalpojumus (piemēram, datu infrastruktūras un lietojumprogrammu pārvaldīšana pie klienta vai no saviem datu centriem).

Atea arī ir jābūt spēkā esošam datu apstrādes līgumam ar jebkuru apakšuzņēmēju un pārdēvēju, kas apstrādā datus Atea vārdā (piemēram, sniedz programmatūras lietojumprogrammu un datu glabāšanas pakalpojumus, kas darbojas pārdevēja datu centrā, piemēram, mākoņpakalpojumus).

Datu aizsardzības pārkāpuma gadījumā, kura rezultātā var tikt veikts kaitējums indivīdam, Atea pienākums ir 72 stundu laikā pēc tam, kad tas ir uzzinājis par pārkāpumu, ziņot tās valsts uzraudzības iestādei, kurā pārkāpums noticis.

3. ATEA DATU AIZSARDZĪBAS POLITIKA

Veicot datu apkopošanu, apstrādi un izplatīšanu, Atea darbiniekiem ir vienmēr jāievēro uzņēmuma datu aizsardzības politika. Visu Atea vadītāju pienākums ir nodrošināt, ka viņu atbildības jomā notiekošajos biznesa procesos tiek ievērota Atea datu aizsardzības politika un ka viņu darbinieki ievēro šos biznesa procesus.

Visiem Atea vadītājiem ir norīkots datu aizsardzības administrators, kurš ir atbildīgs par konkrētu uzņēmējdarbības funkciju savā valstī (vai kopīgu pakalpojumu vienībā). Datu aizsardzības administratora uzdevums ir pārbaudīt, vai visi biznesa procesi, kas ir to uzņēmējdarbības funkciju ietvaros, noris saskaņā ar Atea datu aizsardzības politiku. Šīs funkcijas ir: Pārdošana/mārketings, cilvēkresursi, finanses, konsultāciju pakalpojumi, lietojumprogrammu pārvaldības pakalpojumi, loģistika un IT.

Datu aizsardzības administrators par katru uzņēmējdarbības funkciju ziņo valsts (vai kopīgas pakalpojumu vienības) informācijas sistēmu drošības pārvaldniekam. Katras valsts informācijas sistēmu drošības pārvaldniekam ir vispārēja atbildība par datu aizsardzības politikas īstenošanu šajā valstī, un tas ziņo grupas informācijas sistēmu drošības pārvaldniekam.

Visu jūsu valsts Informācijas sistēmu drošības organizācijas pārstāvju kontaktinformāciju iespējams atrast Atea atbilstības tīmekļa vietnē: atea.com/trust. Šā dokumenta pielikumā ir pievienots arī Informācijas sistēmu drošības organizācijas pārskats.

Atea datu aizsardzības politika aptver:

- Sistēmu reģistrāciju
- Datu klasifikāciju
- Personas datu pārvaldību
- Klientu līgumus

Datu aizsardzības politikas pārskats:

Sistēmu reģistrācija

Pirms Atea darbinieki uzsāk informācijas apkopošanu, apstrādi vai izplatīšanu, viņiem ir jāpārliecinās, ka visas informācijas sistēmas, kurās informācija tiks uzglabāta vai apstrādāta, ir reģistrējis un apstiprinājis attiecīgās valsts informācijas sistēmu drošības pārvaldnieks. Tas ietver arī jebkuru ar abonentu iegādātu mākoņpakalpojumu, kurš tiek pārvaldīts ārpus Atea.

Pirms sistēmas reģistrācijas un apstiprināšanas lietošanai informācijas sistēmu drošības pārvaldnieks veiks informācijas sistēmas IT drošības un datu privātuma standartu analīzi. Analīze balstās uz Atea IT drošības un datu aizsardzības standartu kontrolsarakstu, un tā tiek veikta kopā ar Atea grupas informācijas sistēmu drošības pārvaldnieku.

Analizējot, vai sistēma atbilst Atea informācijas sistēmu drošības prasībām, informācijas sistēmu drošības pārvaldnieks arī noteiks sistēmā glabājamo datu veidu un sensitivitātes līmeni. Veicot analīzi, informācijas sistēmu drošības pārvaldnieks apstiprinās arī sistēmas personas datu dzēšanas politiku, kad tā Atea vairāk nav nepieciešama („datu samazināšanas" politika).

Ja informācijas sistēma tiek pārvaldīta ar ārpakalpojumu un tajā glabājas personas dati, piemēram, personālvadības sistēmas mākoņpakalpojums, lai ievērotu GDPR, Atea ar pakalpojuma sniedzēju ir jābūt parakstītam datu apstrādes līgumam. Standarta datu apstrādes līgums ar mākoņpakalpojumu sniedzēju ir pieejams jūsu valsts iekštīkla globālajā informācijas drošības tīmekļa vietnē. Katras valsts informācijas sistēmu drošības pārvaldnieks var atbildēt uz jautājumiem par datu apstrādes līgumu un var atbalstīt līguma parakstīšanu ar pakalpojuma sniedzēju.

Atea darbinieki nedrīkst uzglabāt vai apstrādāt uzņēmuma datus „ēnu IT" sistēmās, kuras nav reģistrējis attiecīgās valsts informācijas sistēmu drošības pārvaldnieks. Atea darbinieki nav tiesīgi veikt būtiskas izmaiņas datu apstrādes sistēmās vai procesos, neinformējot par to informācijas sistēmu drošības pārvaldnieku, lai varētu veikt jaunu IT drošības novērtējumu.

Kad sistēma ir apstiprināta Atea iekšienē, tai tiks piešķirts sistēmas pārzinis. Sistēmas pārziņa pienākums būs nodrošināt, ka sistēma tiek izmantota saskaņā ar Atea datu aizsardzības politiku. It īpaši sistēmas pārzinis ir atbildīgs par to, lai piekļuves tiesības informācijas sistēmai būtu ierobežotas tikai tām personām, kurām ir nepie-

ciešams zināt attiecīgo informāciju, un tās tiktu pārtrauktas, tiklīdz tas vairs nav nepieciešamas. Sistēmas pārzinis ir atbildīgs par to, ka mirklī, kad Atea vairs nav nepieciešami personas dati, tie tiktu izdzēsti no sistēmas saskaņā ar datu samazināšanas politiku, kas ir apstiprināta līdz ar sistēmas reģistrēšanu.

Datu klasifikācija

Kad sistēma tiek autorizēta izmantošanai Atea, tiks dokumentēts sistēmā uzglabāto datu veids un sensitivitātes līmenis, lai nodrošinātu atbilstošu datu aizsardzības politiku ievērošanu.

Tomēr, daudzos gadījumos Atea darbinieki apstrādās un izplatīs informāciju ārpus autorizētās IT sistēmas. Tas ietver informāciju, kas tiek apstrādāta, izmantojot drukātus dokumentus, e-pastu vai koplietojot failu (t.i., Microsoft Word/Excel/Powerpoint failu).

Lai nodrošinātu, ka informācija, kas atrodas ārpus autorizētas IT sistēmas, tiktu pārvaldīta atbilstošā informācijas drošības līmenī, Atea darbinieku pienākums ir īpaši atzīmēt jebkuru datni, dokumentu vai e-pastu, kas satur informāciju, atbilstoši tā sensitivitātes līmenim, lai informācijas saņēmējs to saprastu. Informācija ir jāatzīmē saskaņā ar Atea datu klasifikācijas standartiem.

Atea datu klasifikācijas standartiem ir pieci līmeņi, kas klasificē e-pastā vai datnē glabāto informāciju no zemākā sensitivitātes līmeņa līdz visaugstākajam. Klasifikācijas standarti ir iestrādāti Atea Microsoft Outlook un Word/Excel/Powerpoint versijās. Atea darbinieki var automātiski atzīmēt e-pastu, dokumentu vai datni ar pareizo datu klasifikācijas marķējumu, izvēloties pogu šo programmatūru galvenē.

Pieci līmeņi ir šādi:

1. Ar uzņēmējdarbību nesaistīta informācija: Privātas e-pasta sarakstes un dokumenti, kas nav saistīti ar Atea

2. Publiska informācija: Ar Atea saistīta informācija, kuru drīkst izplatīt publiski

3. Iekšēja informācija: Informācija, kuru drīkst brīvi izplatīt Atea struktūrvienībās un līgumattiecībās esošajiem trešo pušu piegādātājiem. To nav paredzēts izplatīt ārpus Atea vai citiem, kas nav Atea līgumiskas partneris.

4. Konfidenciāla informācija:
Informācija, kas saņēmējam ir jāglabā privāti, un to nedrīkst koplietot bez informācijas īpašnieka apstiprinājuma. Tas ietver personas datus, kas būtu jānorāda atsevišķi. Personas datu marķējumu var pievienot, izmantojot nolaižamo izvēlni zem pogas „Confidential" (Konfidenciāli).

5. Augstākā līmeņa konfidenciāla informācija:
Informācija, kuru izplatot bez autorizācijas, Atea piedzīvotu būtiskas negatīvas sekas. Informācija ir jāglabā šifrētā formātā, un to nedrīkst koplietot bez informācijas īpašnieka apstiprinājuma. Iekļauj:

- Sensitīvus personas datus: Saskaņā ar GDPR īpašas personas datu kategorijas ir jāapstrādā, veicot papildu drošības pasākumus. Tas ietver informāciju, kas saistīta ar: etnisko izcelsmi, politiskajiem uzskatiem, reliģiju, dalību arodbiedrībās un ģenētiskajiem vai biometriskajiem datiem. Sensitīvos personas datus būtu jānorāda atsevišķi. Šo marķējumu var pievienot, izmantojot nolaižamo izvēlni zem pogas „Strictly confidential" (īpaši konfidenciāli).
- Sensitīvu biznesa informāciju: Tā ietver konfidenciālu uzņēmējdarbības informāciju, piemēram, klienta vai piegādātāja datus, līgumus un komerciālus noteikumus. Tajā ir iekļauta arī informācija, kas ir ietverta konfidencialitātes līgumā ar klientu vai darījumu partneri. Visbeidzot, tas var ietvert īpaši sensitīvu intelektuālo īpašumu, piemēram, uzņēmējdarbības koncepcijas un iekšēji izstrādātu programmatūru, metodoloģijas un rīkus.
- Cenas jutīga informāciju: Cenas jutīga informācija ir īpašs konfidenciālas informācijas veids, kas var ietekmēt Atea akciju cenu. Tā ietver nozīmīgus finanšu datus, par kuriem vēl nav ziņots, vai konfidenciālu sarunu statusu saistībā ar ļoti lielu klientu līgumu vai tirdzniecības nolīgumu.
- Atea vadītājs ir nekavējoties jāinformē par visiem darbiniekiem, kuru rīcībā ir cenas jutīga informācija. Šie darbinieki tiks reģistrēti iekšējā datordalīšanās pārvaldības sistēmā („Computershare Insider Management System" (CIMS)), ko izmanto Atea. Papildu informācija par cenu jutīgas informācijas atbilstības procedūrām atrodama Rīcības kodeksā.

Pilns Atea datu klasifikācijas standartu apraksts, kā arī dokumentu un e-pasta ziņojumu marķēšanas un šifrēšanas procedūras ir atrodamas jūsu valsts iekštīkla globālajā informācijas drošības tīmekļa vietnē.

Personas datu pārvaldība

Saskaņā ar GDPR, Atea ir īpašas juridiskas saistības, apstrādājot personas datus – informāciju, kas var būt saistīta ar konkrētu un identificējamu personu. Šīs juridiskās saistības uzliek Atea par pienākumu dokumentēt, ka tas ir veicis pietiekamus tehniskus un organizatoriskus pasākumus, lai izpildītu GDPR prasības. Šā procesa dokumentācija pēc pieprasījuma ir jādara pieejama valsts iestādēm.

Pirms Atea var uzsākt personas datu apkopošanu, biznesa procesam, ar kuru jāapstrādā personas dati, jābūt pilnībā dokumentētam un informācijas sistēmu drošības pārvaldnieka pārskatītam. Katras funkcijas datu aizsardzības administrators ir atbildīgs par to, lai visi personas datu apstrādes procesi to funkciju ietvaros būtu dokumentēti un atjaunināti saskaņā ar GDPR.

Dokumentācijai ir jāspēj pierādīt, ka Atea ir veicis pietiekamus tehniskus un organizatoriskus pasākumus, lai ievērotu indivīda tiesības uz personas datiem, novērstu un samazinātu datu aizsardzības pārkāpuma ietekmi un lai likumīgi reaģētu personas datu aizsardzības pārkāpuma gadījumā. Personas datu apkopošanas procesos jāiekļauj arī datu samazināšanas procedūra, t.i., personas datu dzēšana, ja tie vairs nav vajadzīgi.

Apkopojot datus, Atea pienākums ir informēt personu vai jāsaņem viņa/-as piekrišana, ka viņa/-as personas dati tiek apkopoti un izmantoti. Saskaņā ar GDPR, informējot personu vai iegūstot piekrišanu, Atea ir jāsniedz šāda informācija:

1. Apkopoto un apstrādājamo personas datu kategorijas
2. Datu apstrādes mērķis un juridiskais pamatojums
3. Personas datu saņēmēji vai saņēmēju kategorijas
4. Periods, kurā dati tiks izmantoti, vai kritēriji, kas izbeidz šo periodu
5. Indivīda tiesības uz personas datiem, ieskaitot tiesības atsaukt piekrišanu un tiem piekļūt, izdzēst un labot
6. Indivīda tiesības sūdzēties uzraudzības iestādē.
7. Vajadzības gadījumā paziņojums par to, ka dati tiks pārsūtīti uz citu valsti, un apstiprinājums, ka datu apstrāde citā valstī būs saskaņā ar GDPR noteikumiem par datu aizsardzības pietiekamību
8. Ja tiek apkopoti sensitīvi personas dati, Atea ir jāpieprasa un jāsaņem nepārprotama piekrišana no personas, kuras dati tiek apstrādāti.

Standarta paziņojums par konfidencialitāti nolūkam apkopot personas datus ir pieejams jūsu valsts iekštīkla globālajā informācijas drošības tīmekļa vietnē.

Saskaņā ar GDPR Atea ir īpašas saistības datu aizsardzības pārkāpuma gadījumā, kurā iesaistīti personas dati. Datu drošības pārkāpums ir informācijas sistēmu drošības incidents, kā rezultātā nepiederošas personas iegūst piekļuvi datiem vai izraisa datu nelikumīgu vai nejaušu nozaudēšanu.

Datu drošības pārkāpuma gadījumā Atea darbinieku pienākums ir nekavējoties paziņot par to valsts vai kopīgas pakalpojumu vienības informācijas sistēmu drošības pārvaldniekam. Informācijas sistēmu drošības pārvaldnieks izmeklēs datu aizsardzības pārkāpumu kopā ar Atea Informācijas sistēmu drošības organizāciju un nepieciešamības gadījumā veiks korektīvus pasākumus, lai ziņotu par jebkādiem zaudējumiem un mazinātu tos, ko radījis datu aizsardzības pārkāpums.

Datu aizsardzības pārkāpuma gadījumā, kura rezultātā var tikt veikts kaitējums indivīdam, Atea pienākums ir 72 stundu laikā pēc tam, kad tas ir uzzinājis par pārkāpumu, ziņot tās valsts uzraudzības iestādei, kurā pārkāpums noticis. Paziņojumā jāapraksta pārkāpuma veids, skarto datu subjektu un attiecīgo dokumentu kopsavilkums, pārkāpuma iespējamās sekas un veiktie pretpasākumi.

Ja personai, kuru personas datu aizsardzība ir pārkāpta, pastāv liels kaitējuma risks, viņš/-a ir nekavējoties jāinformē par pārkāpumu. Ja individuāls paziņojums nav iespējams, ir pietiekams publisks paziņojums.

Klientu līgumi

Atea pārvalda daudzu klientu datu infrastruktūras un lietojumprogrammas, vai nu klienta atrašanās vietā, vai arī no saviem datu centriem. Šajos gadījumos Atea ir līgumiski atbildīgs par klienta datu

apstrādi, un tam ir juridisks pienākums saskaņā ar GDPR nodrošināt, ka tas pienācīgi aizsargās to personu privātuma tiesības, kuru personas dati ir iekļauti klienta datos.

Saskaņā ar GDPR noteikumiem, pārvaldot klienta datu infrastruktūru un lietojumprogrammas, Atea ar klientiem ir jābūt noslēgtam datu apstrādes līgumam. Datu apstrādes līgumā ir jāiekļauj Atea veikto datu apstrādes darbību jomu, raksturu un ilgumu, ko Atea veic saskaņā ar klienta instrukcijām. Dokumentācijā ir jāiekļauj arī kopsavilkums, kuru veidu personas datus Atea apstrādās klienta vārdā un kuru kategoriju personas dati tiks apstrādāti.

Saskaņā ar GDPR datu apstrādes līgumā ir jāiekļauj šāda Atea informācija:

1. Atea apstrādā personas datus tikai ar dokumentētiem klienta norādījumiem un ievēro datu aizsardzības likumus
2. Atea darbinieki, kas apstrādā personas datus, ir apņēmušies ievērot konfidencialitāti. Atea nenorīkos apakšuzņēmējus, lai apstrādātu klienta personas datus, bez klienta atļaujas.
3. Atea ir veicis pietiekamus tehniskus un organizatoriskus pasākumus, lai nodrošinātu ar klientu saskaņotu drošības līmeni atbilstoši apstrādājamo datu riskam.
4. Atea ir veicis pietiekamus pasākumus, lai izpildītu savas juridiskās saistības attiecībā uz personu tiesībām kontrolēt savu datu apstrādi, kā aprakstīts GDPR
5. Atea sniegs klientam visu nepieciešamo informāciju, lai pierādītu atbilstību GDPR noteiktajiem datu privātuma pienākumiem, un pēc pieprasījuma piedalīsies klienta atbilstības revīzijā
6. Atea bez liekas kavēšanās informēs klientu par personas datu aizsardzības pārkāpumiem
7. Atea pakalpojuma līguma beigās izdzēsīs vai atgriezīs klientam visus personas datus

Atea izmanto ārējo apakšuzņēmēju pakalpojumus, lai izpildītu savus datu apstrādes pienākumus pret klientu (piemēram, trešo personu mākoņpakalpojumus, konsultantus vai infrastruktūras nodrošinātājus); Atea ir jābūt ar šo apakšuzņēmēju noslēgtam atsevišķam datu apstrādes līgumam, kurā apakšuzņēmējs sniedz līdzīgu apstiprinājumu kā iepriekšējie apliecinājumi.

Atea ir izstrādāts standarta datu apstrādes līgums, kuru ir ieteicams izmantot, slēdzot līgumus ar visiem klientiem un apakšuzņēmējiem. Datu apstrādes līgums ir pieejams jūsu valsts iekštīkla globālajā informācijas drošības tīmekļa vietnē. Katras valsts informācijas sistēmu drošības pārvaldnieks var atbildēt uz jautājumiem par datu apstrādes līgumu un var atbalstīt līguma parakstīšanu ar klientu vai apakšuzņēmēju.

Personas datu aizsardzības pārkāpuma gadījumā, kurā ir iesaistīti klientu dati, Atea pienākums ir nekavējoties paziņot klientam par datu aizsardzības pārkāpumu tiklīdz tas ir konstatēts. Atea ir jāsadarbojas ar savu klientu un jāveic saprātīgi pasākumi, lai nodrošinātu, ka klients var izpildīt savu pienākumu ziņot par datu aizsardzības pārkāpumiem, kā to pieprasa GDPR, un var veikt korektīvus pasākumus, lai mazinātu pārkāpuma radītos zaudējumus.

Būtiskākie fakti:

Sistēmu reģistrācija

Visas izmantotās sistēmas ir jāreģistrē tās valsts vai kopīgas pakalpojumu vienības informācijas sistēmu drošības pārvaldniekam, kurā tiek izmantota sistēma. Tas ietver ar abonentu iegādātu mākoņpakalpojumu, kurš tiek pārvaldīts ārpus Atea.

Pirms sistēmas apstiprināšanas lietošanai informācijas sistēmu drošības pārvaldnieks veiks IT sistēmas analīzi, lai pārliecinātos, ka tā atbilst Atea IT drošības standartiem. Tiklīdz sistēma tiks reģistrēta, tai tiks norīkots sistēmas pārzinis. Sistēmas pārziņa uzdevums ir nodrošināt, ka sistēma tiek izmantota saskaņā ar Atea datu aizsardzības politiku, īpaši pievēršot uzmanību piekļuves tiesību pārvaldīšanai.

Datu klasifikācija

Lai nodrošinātu, ka informācija, kas atrodas ārpus autorizētas IT sistēmas, tiktu pārvaldīta atbilstošā informācijas drošības līmenī, Atea darbinieku pienākums ir īpaši atzīmēt jebkuru datni, dokumentu vai e-pastu, kas satur informāciju, atbilstoši tā sensitivitātes līmenim, lai to saprastu visi informācijas saņēmēji. Informācija ir jāatzīmē saskaņā ar Atea datu klasifikācijas standartiem.

Visām personas datu apstrādes kārtībām ir jābūt dokumentētām un informācijas sistēmu drošības pārvaldnieka pārskatītām. Visiem Atea vadītājiem ir norīkots datu aizsardzības administrators, kurš ir atbildīgs par konkrētu uzņēmējdarbības funkciju savā valstī (vai kopīgu pakalpojumu vienībā). Datu aizsardzības administratora uzdevums ir pārbaudīt, vai visi biznesa procesi, kas ir to uzņēmējdarbības funkciju ietvaros, noris saskaņā ar Atea datu aizsardzības politiku un GDPR prasībām.

Personas datu pārvaldība

Apkopojot datus, saskaņā ar GDPR Atea pienākums ir informēt personu vai jāsaņem viņa/-as piekrišana, ka viņa/-as personas dati tiek apkopoti un izmantoti. GDPR ir daudz informācijas prasību attiecībā uz paziņojuma saturu (sk. galveno tekstu).

Datu drošības pārkāpums ir informācijas sistēmu drošības incidents, kā rezultātā nepiederošas personas iegūst piekļuvi datiem vai izraisa datu nelikumīgu vai nejaušu nozaudēšanu. Saskaņā ar GDPR Atea ir īpašas saistības datu aizsardzības pārkāpuma gadījumā, kurā iesaistīti personas dati.

Aizdomu gadījumā par datu aizsardzības pārkāpumu Atea darbinieku pienākums ir nekavējoties paziņot par to valsts vai kopīgas pakalpojumu vienības informācijas sistēmu drošības pārvaldniekam. Iespējams arī nosūtīt e-pasta ziņojumu uz infosec@atea.com, kas tiks novirzīts Atea grupas informācijas sistēmu drošības pārvaldniekam.

Saskaņā ar GDPR noteikumiem, pārvaldot klienta datu infrastruktūru un lietojumprogrammas, Atea ar klientiem ir jābūt spēkā esošam datu apstrādes līgumam. Tāpat Atea ir jābūt spēkā esošam datu apstrādes līgumam ar apakšuzņēmējiem vai pārdevējiem, kuri Atea vārdā apstrādā datus. GDPR ir daudz informācijas prasību attiecībā uz datu apstrādes līgumu (sk. galveno tekstu).

4. IT INFRASTRUKTŪRAS DROŠĪBA - OBLIGĀTAS PRAKSES VISIEM DARBINIEKIEM

Atea IT infrastruktūra sastāv no visām aparatūras, programmatūras un tīkla sastāvdaļām, kas atbalsta biznesa sistēmu un IT iespējotu procesu piegādi lietotājiem. Datu aizsardzība Atea ir atkarīga no visiem darbiniekiem, kuri godprātīgi izmanto Atea IT infrastruktūras aktīvus.

Turpmākā politika attiecas uz visiem Atea darbiniekiem kā Atea IT infrastruktūras lietotājiem, un tā aptver ierīces drošību, piekļuvi sistēmai, datņu glabāšanu, tīkla drošību, sakarus un fizisko drošību. Papildus tam, darbiniekiem, kuru pienākumos ir Atea IT darbību pārvaldība, ir jāveic atsevišķa, plašāka apmācība par IT drošību, kas atbilst viņu funkcijām.

Ierīces drošība:
Atea darbiniekiem, lietojot savas ierīces, piemēram, datorus, planšetdatorus un viedtālruņus, ir jāievēro drošības pasākumi. Šīs ierīces ir pakļautas zādzībām, ļaunprogrammatūrām un neautorizētai lietošanai. Atea datori, planšetdatori un viedtālruņi vienmēr ir jāuzmana vai jāglabā drošā vietā. Kad tās netiek izmantotas, tās ir jāaizsargā ar PIN/paroli vai jāizslēdz.

Visos Atea datoros, planšetdatoros un viedtālruņos jābūt instalētiem šifrēšanas risinājumiem, lai novērstu neautorizētu piekļuvi cietajam diskam. Atea Windows datori tiek aktivizēti ar Bitlocker šifrēšanas risinājumu. Apple Mac modeļos nav instalēta diska šifrēšanas funkcija, tāpēc tā ir jāaktivizē lietošanas laikā. Visās iPhone un iPad ierīcēs ir iepriekš uzstādīta šifrēšanas funkcija. Android mobilajos telefonos un planšetdatoros šifrēšanas funkcija ir jāiespējo manuāli. Šifrēšanas funkcija ir jāaktivizē arī ārējā atmiņā, piemēram, USB, kuru var viegli pazaudēt. Darbinieki, kuriem ir nepieciešama palīdzība savu darba ierīču šifrēšanā, var vērsties pie Atea Servicedesk pārstāvjiem.

Atea darbiniekiem nevajadzētu savos datoros lejupielādēt programmatūras, kuras nav nodrošinājis Atea IT departaments. Atea IT departaments piedāvā daudzas programmatūras, izmantojot tā portālu „Accelerator". Lai nodrošinātu atbilstošu drošības līmeni, šīs lietojumprogrammas tiek regulāri atjauninātas. Ja Atea darbiniekam ir nepieciešams savā datorā lejupielādēt ārējo programmatūru, kas nav no „Accelerator" portāla, viņam/-ai vispirms ir jāsaņem apstiprinājums no sava vadītāja un vietējās IT organizācijas.

Atea datoros ir iepriekš instalētas pretvīrusu un ugunsmūra lietojumprogrammas. Ja jums ir šaubas par pretvīrusu aizsardzību, sazinieties ar Atea Servicedesk. Ja saņemat pretvīrusu programmas brīdinājumu vai ja jūsu dators darbojas neparasti, tā var būt pazīme, ka jūsu dators ir apdraudēts. Ļaunprogrammatūras pazīmes datorā var ietvert biežu darbības apstāšanos vai neparasti lēnu apstrādi, vai darbības, kas notiek bez uzsākšanas, ieskaitot uznirstošos logus vai citas izmaiņas ekrānā.

Ja rodas aizdomas, ka jūsu dators ir apdraudēts, vispirms pārtrauciet darbu ar datoru un atvienojiet to no tīkla. Pēc tam sazinieties ar Atea Servicesk un sniedziet informāciju par to, kādi simptomi ir radījuši aizdomas par to, ka datoram ir uzbrukts ar ļaunprogrammatūru, un kādi notikumi varēja novest pie datora bojājuma.

Visas darba ierīces, kuras ir izņemtas no aprites, pirms nosūtīt Atea birojam uz apkopi, pārstrādi vai atkārtotu izmantošanu, ir vispirms jāiztīra no visiem datiem. Tas jādara saskaņā ar katrā valstī ieviestajām IT procedūrām. Šīs procedūras ir pieejamas jūsu valsts iekštīkla globālajā informācijas drošības tīmekļa vietnē.

Piekļuve sistēmai:
Atea darbiniekiem jāpiešķir piekļuve sistēmām tikai tad, ja tas ir nepieciešams viņu tiešo pienākumu veikšanai. Lai nodrošinātu šīs politikas noteikumu ievērošanu, ir pastāvīgi jāpārbauda sistēmu piekļuves tiesības, un tās jāpārtrauc, tiklīdz tās vairs nav nepieciešamas. Ja Atea darbiniekam ir piekļuve sistēmām, kas tām vairs nav nepieciešamas, viņam nekavējoties jāsazinās ar sistēmas pārzini, lai izbeigtu piekļuves tiesības.

Kad Atea darbiniekam ir piešķirtas piekļuves tiesības sistēmai, lietotāja vārds un pagaidu parole ir jāglabā atsevišķi. Pagaidu parole ir nekavējoties jānomaina pēc pirmā pieteikšanās, un to nedrīkst pierakstīt vai ar kādu koplietot. Darbinieki nedrīkst izsniegt piekļuves tiesības citiem lietotājiem.

Datņu uzglabāšana:
Visi Atea darbinieki ir atbildīgi par to, lai viņu darba datnes (piemēram, MS Word/Excel/Powerpoint datnes) tiktu droši pārvaldītas. Visi datņu veidi ir jāglabā uz Atea iekšējiem koplietošanas serveriem, OneDrive kontos vai Sharepoint vidē. Lai glabātu Atea datnes, citas glabātuves, tajā skaitā Dropbox vai Google Drive, nedrīkst izmantot bez atklātas attiecīgās valsts IT departamenta atļaujas, jo Atea nevar garantēt šo glabātavu drošību. Atea darbiniekiem nevajadzētu glabāt informāciju par uzņēmuma ārējos cietajos diskos, jo šī informācija netiek automātiski dublēta, un tāpēc ir iespējams datu zudums.

Datnes ir jāapzīmē saskaņā ar Atea datu klasifikācijas standartiem (5 līmeņi). Datnes ar augstākā līmeņa konfidencialitātes atzīmi ir jāglabā šifrētā formātā. Datnēm, kas satur personas datus, jābūt arī marķētām un glabātām saskaņā ar GDPR.

Atea darbiniekiem ir jābūt ļoti piesardzīgiem, glabājot personas datus datnēs, ņemot vērā GDPR stingras datu privātuma prasības. Darbinieki nedrīkst izmantot personas datus ārpus sākotnējā mērķa, kas tika definēts un paziņots personai, kuras dati ir apkopoti. Darbiniekiem ir jāierobežo tādu datņu koplietošana, kas satur personas datus, lai novērstu šo datu aizsardzības pārkāpumus vai ļaunprātīgu izmantošanu, un jāizdzēš personas dati, tiklīdz tie vairs nav vajadzīgs. Tas attiecas uz visām Atea darbinieku radītajām datnēm, ieskaitot MS Word/Excel/Powerpoint datnes.

Tīkla drošība:
ATEA domēnam drīkst pieslēgties tikai Atea klienti (datori, kas ir konfigurēti saskaņā ar Atea standartiem). Atea mobilās ierīces pievienosies tikai Atea WiFi tīklam, kas paredzēts mobilajām ierīcēm. Citi datori vai mobilās ierīces tiks novirzītas uz ATEA-guest WiFi (viesu) tīklu.

Atea piedāvā darbiniekiem, kas atrodas ārpus biroja, iespēju izveidot savienojumu ar iekšējo tīklu, izmantojot Cisco VPN vai Citrix. Tas ļauj piekļūt mūsu kopējai datņu sistēmai, kā arī mūsu kopējām biznesa lietojumprogrammām. Lai izveidotu savienojumu ar Cisco VPN, datoram ir jābūt Atea īpašumā, ir jābūt Atea domēna (ONE) biedram un jābūt instalētai pretvīrusu programmatūrai.

Atea darbiniekiem nekad nevajadzētu pieslēgties klienta tīklam bez klienta iepriekšējas piekrišanas, ja vien klienta līgumā nav noteikts citādi. Klients būtu jāinformē ikreiz, kad Atea darbinieks pieslēdzas viņu tīklam, un katru reizi Atea darbiniekam ir jāziņo par darbībām, kādas ir veiktas, izmantojot klienta tīklu.

Atea darbiniekiem ir jāuzmanās, ceļojumu laikā lietojot publiski pieejamus WiFi tīklus. Publiskajos tīklos iespējams kontrolēt datu plūsmu. Pirms pieslēgšanās WiFi tīklam Atea darbiniekam ir jāpārliecinās, ka tīkls ir drošs un to nodrošina likumīgs pakalpojuma sniedzējs. Ja ir pamats šaubām par publiskā WiFi drošību, Atea darbiniekam tā vietā ir jāizmanto mobilo sakaru tīkls. Atea Servicedesk var sniegt atbalstu datora pieslēgšanai mobilo sakaru tīklam.

Atea darbiniekiem internets ir jāizmanto ikdienas darba vajadzībām. Pārlūkošana privātām vajadzībām ir atļauta, bet tā var būt iespējama tikai tādās vietnēs, kuru saturs ir piemērots darbavietai. Tiešsaistes spēļu vai azartspēļu spēlēšana nav atļauta, un datņu koplietošanai vai mediju straumēšanai, izmantojot internetu, vajadzētu būt tikai ar darbu saistītās vajadzībās. Visiem darbiniekiem ir jābūt informētiem, ka Atea analizē interneta datu plūsmu, lai konstatētu uzbrukumus Atea tīklam, kā arī tādējādi tiks konstatēta nepiemērota interneta lietošana.

Piekļūstot tīmekļa lapām internetā, esiet piesardzīgs, lai tīmekļa lapa būtu precīza - it īpaši, ja esat novirzīts no citas lapas. Nekad neklikšķiniet uz saites vai uznirstošajiem logiem tīmekļa lapās, ja tās šķiet aizdomīgas, jo tajās var būt ļaunprogrammatūras, kuras var ielādēt ierīcē.

Komunikācija (e-pasts/sociālie tīkli):
Atea darbiniekiem e-pasts ir svarīgs digitālās komunikācijas rīks. Tas ir arī galvenais informācijas aizsardzības pārkāpumu avots, jo tas sniedz krāpniekiem iespēju uzbrukt Atea ar ļaunprogrammatūru, krāpšanu un citiem draudiem ar zemām izmaksām un zemu kriminālvajāšanas risku.

Viens identitātes viltošanas (pikšķerēšanas) veids ir krāpnieku sazināšanās ar Atea darbiniekiem, izmantojot e-pasta ziņojumus. Šis e-pasta ziņojums ir no šķietami uzticama avota, bieži vien izmantojot viltus identitāti, piemēram, cita Atea darbinieka, biznesa partnera vai pakalpojumu sniedzēja (tehnoloģiju uzņēmuma vai bankas). E-pasta ziņojuma mērķis ir panākt Atea darbinieka atbildes darbību, piemēram, naudas pārskaitīšanu, pieteikšanās/paroles vai sensitīvu datu ievadīšanu vai klikšķināšanu uz saites vai pielikuma, kurš lietotāja datorā vai mobilajā telefonā lejupielādē ļaunprogrammatūru.

E-pasts, pielikums vai saite ir šķietami nekaitīgi - piemēram, tie ir maskēti kā vēstule no kolēģa, piedāvājums/rēķins no pārdevēja vai kā paziņojums no mākoņpakalpojuma konta, piemēram, OneDrive. Šā iemesla dēļ Atea darbiniekiem ir jābūt ļoti uzmanīgiem un jāizvērtē jebkurš e-pasts vai cita veida saziņa pret krāpšanas iespējamību, pat ja paziņojums šķiet no uzticama avota.

Atea darbiniekiem nekad nevajadzētu atvērt saites vai pielikumus, izmantojot savas ierīces, ja viņiem ir šaubas par e-pasta vai komunikācijas leģitimitāti. Ja Atea darbinieks nav pārliecināts par e-pasta leģitimitāti vai, ja darbinieks nejauši ir reaģējis uz iespējamu krāpšanas mēģinājumu, atverot aizdomīgu saiti vai pielikumu, viņa pienākums ir nekavējoties sazināties ar Atea Servicedesk un ziņot par iespējamu apdraudējumu.

Darbinieku e-pasta konti ir biežs uzbrucēju mērķis, kuri cenšas piekļūt darbinieka konfidenciālām uzņēmuma datnēm. Šā iemesla dēļ e-pastu nedrīkst izmantot svarīgas uzņēmējdarbības informācijas glabāšanai. Uzņēmējdarbības informācija jāglabā vai jāizplata, izmantojot drošas biznesa sistēmas vai failu koplietošanas risinājumus, nevis e-pastu.

E-pasta izmantošana privātām vajadzībām ir atļauta, ja vien tā nav pretrunā ar Atea biznesa interesēm vai netraucē darbam. Privātajai e-pasta korespondencei vienmēr jābūt darbavietai atbilstošai, un tai jābūt atzīmētai „ Non-business" (ar uzņēmējdarbību nesaistīts). Turklāt uzņēmuma e-pasta konta izmantošana personīgai komunikācijai nedrīkst atstāt iespaidu, ka korespondence ir Atea rīcībā vai to ir apstiprinājis uzņēmums.

Sociālie mediji ir arī bieži sastopams saziņas līdzeklis Atea darbinieku vidū. Ja tie ir izmantoti atbilstoši, sociālie mediji sniedz Atea darbiniekiem iespēju iegūt zināšanas un nodot tās tālāk, veidot komerciālas attiecības un stiprināt Atea zīmolu. No otras puses, ja sociālie mediji tiek izmantoti neatbilstoši vai ja tiek kopīgota sensitīva informācija, tie var ievērojami kaitēt Atea un tā darbiniekiem.

Tādēļ Atea darbiniekiem ir jābūt ļoti piesardzīgiem attiecībā uz to, kādu informāciju viņi koplieto sociālajos medijos. Jebkuri personas dati (ieskaitot vārdus, attēlus u.c.) var tikt koplietoti sociālo mediju ierakstos, kas saistīti ar Atea uzņēmējdarbību, tikai tādā gadījumā, ja persona, kuras dati tiks koplietoti, tam piekrīt.

Drošība birojā:

Atea darbiniekiem jāvalkā drošības nozīmītes, lai viņus būtu iespējams identificēt. Visiem Atea apmeklētājiem ir jāreģistrējas reģistratūrā, un viņiem ir jāizsniedz apmeklētāja nozīmīte, kas ir jātur redzamā vietā. Apmeklētāji ir jāsagaida reģistratūrā apmeklējuma sākumā un jāpavada līdz reģistratūrai, lai pēc apmeklējuma beigām atgrieztu nozīmīti. Apmeklētājus Atea telpās nedrīkst atstāt vienus.

Visa sensitīvā informācija ir jānoņem no galdiem un droši jāglabā, kad tā netiek izmantota. Visas tāfeles sanāksmju beigās ir jānotīra. Konfidenciāliem dokumentiem vienmēr jābūt iznīcinātiem dokumentu smalcinātājos vai izmetot īpašās privātuma dokumentu likvidēšanas tvertnēs, kad tie vairs nav nepieciešami.

Būtiskākie fakti – IT infrastruktūras drošība

Ierīces drošība:
Visos Atea datoros, planšetdatoros un viedtālruņos jābūt instalētiem šifrēšanas risinājumiem, lai novērstu neautorizētu piekļuvi cietajam diskam. Atea datori, planšetdatori un viedtālruņi vienmēr ir jāuzmana vai jāglabā drošā vietā. Kad tās netiek izmantotas, tās ir jāaizsargā ar PIN/paroli vai jāizslēdz.

Atea darbiniekiem nevajadzētu savos datoros lejupielādēt programmatūras, kuras nav nodrošinājis Atea IT departaments. Ja Atea darbiniekam ir nepieciešams savā datorā lejupielādēt ārējo programmatūru, ko nenodrošina Atea, viņam/-ai vispirms ir jāsaņem apstiprinājums no sava vadītāja un vietējās IT organizācijas.

Atea datoros ir iepriekš instalētas pretvīrusu un ugunsmūra lietojumprogrammas. Ja jums ir šaubas par pretvīrusu aizsardzību, sazinieties ar Atea Servicedesk.

Ja rodas aizdomas, ka jūsu dators ir inficēts ar ļaunprogrammatūru, vispirms pārtrauciet darbu ar datoru un atvienojiet to no tīkla. Pēc tam sazinieties ar Atea Servicedesk.

Piekļuve sistēmai:
Atea darbiniekiem jāpiešķir piekļuve sistēmām tikai tad, ja tas ir nepieciešams viņu tiešo pienākumu veikšanai. Lai nodrošinātu šīs politikas noteikumu ievērošanu, ir pastāvīgi jāpārbauda sistēmu piekļuves tiesības, un tās jāpārtrauc, tiklīdz tās vairs nav nepieciešamas.

Datņu uzglabāšana:
Visi Atea darbinieki ir atbildīgi par to, lai viņu darba datnes (piemēram, MS Word/Excel/Powerpoint datnes) tiktu droši pārvaldītas. Datnes ir jāapzīmē saskaņā ar Atea datu klasifikācijas standartiem (5 līmeņi), izmantojot atsevišķu apzīmējumu datnēm, kas satur personas datus. Datnes ar augstākā līmeņa konfidencialitātes atzīmi ir jāglabā šifrētā formātā.

Visi datņu veidi ir jāglabā uz Atea iekšējiem koplietošanas serveriem, OneDrive kontos vai Sharepoint vidē. Lai glabātu Atea datnes, citas glabātuves, tajā skaitā Dropbox vai Google Drive, nedrīkst izmantot bez atklātas attiecīgās valsts IT departamenta atļaujas. Atea darbiniekiem nevajadzētu uzglabāt uzņēmuma informāciju vietējo ierīču cietajos diskos.

Tīkla drošība:
ATEA domēnam drīkst pieslēgties tikai Atea klienti (datori, kas ir konfigurēti saskaņā ar Atea standartiem). Atea mobilās ierīces pievienosies tikai Atea WiFi tīklam, kas paredzēts mobilajām ierīcēm. Citi datori vai mobilās ierīces tiks novirzītas uz ATEA-guest WiFi (viesu) tīklu.

Atea darbiniekiem ir jāuzmanās, lietojot publiski pieejamus WiFi tīklus. Pirms pieslēgšanās WiFi tīklam Atea darbiniekam ir jāpārliecinās, ka tīkls ir drošs un to nodrošina likumīgs pakalpojuma sniedzējs.

Piekļuve internetam no darba ierīces būtu jāierobežo, atļaujot vietnes ar darbavietai piemērotu saturu. Visiem darbiniekiem ir jābūt informētiem, ka Atea analizē interneta datu plūsmu, lai konstatētu uzbrukumus Atea tīklam, kā arī tādējādi tiks konstatēta nepiemērota interneta lietošana.

Piekļūstot tīmekļa lapām, esiet piesardzīgs, lai tīmekļa lapa būtu precīza - it īpaši, ja esat novirzīts no citas lapas. Nekad neklikšķiniet uz saites vai uznirstošajiem logiem tīmekļa lapās, ja tās šķiet aizdomīgas, jo tajās var būt ļaunprogrammatūras, kuras var ielādēt ierīcē.

Komunikācija (e-pasts/sociālie tīkli):
E-pasts ir arī galvenais informācijas aizsardzības pārkāpumu avots, jo tas sniedz krāpniekiem iespēju uzbrukt Atea ar ļaunprogrammatūru, krāpšanu un citiem draudiem ar zemām izmaksām un zemu kriminālvajāšanas risku.

Viens identitātes viltošanas (pikšķerēšanas) veids ir krāpnieku sazināšanās ar Atea darbiniekiem, izmantojot e-pasta ziņojumus. Šis e-pasta ziņojums ir no šķietami uzticama avota, bieži vien izmantojot viltus identitāti, piemēram, cita Atea darbinieka, biznesa partnera vai pakalpojumu sniedzēja (tehnoloģiju uzņēmuma vai bankas). E-pasta ziņojuma mērķis ir panākt Atea darbinieka atbildes darbību, piemēram, naudas pārskaitīšanu, pieteikšanās/paroles vai sensitīvu datu ievadīšanu vai klikšķināšanu uz saites vai pielikuma, kurš lietotāja datorā vai mobilajā telefonā lejupielādē ļaunprogrammatūru.

Atea darbiniekiem nekad nevajadzētu atvērt saites vai pielikumus, izmantojot savas ierīces, ja viņiem ir šaubas par e-pasta vai komunikācijas leģitimitāti. Ja Atea darbinieks nav pārliecināts par e-pasta leģitimitāti vai, ja darbinieks nejauši ir reaģējis uz iespējamu krāpšanas mēģinājumu, atverot aizdomīgu saiti vai pielikumu, viņa pienākums ir nekavējoties sazināties ar Atea Servicedesk un ziņot par iespējamu apdraudējumu.

E-pasta izmantošana privātām vajadzībām ir atļauta, ja vien tā nav pretrunā ar Atea biznesa interesēm vai netraucē darbam. Privātajai e-pasta korespondencei vienmēr jābūt darbavietai atbilstošai, un tai jābūt atzīmētai „ Non-business" (ar uzņēmējdarbību nesaistīts).

Atea darbiniekiem ir jābūt ļoti piesardzīgiem attiecībā uz to, kādu informāciju viņi koplieto sociālajos medijos saistībā ar Atea. Jebkuri personas dati (ieskaitot vārdus, attēlus u.c.) var tikt koplietoti sociālo mediju ierakstos, kas saistīti ar Atea uzņēmējdarbību, tikai tādā gadījumā, ja persona, kuras dati tiks koplietoti, tam piekrīt.

Drošība birojā:
Atea darbiniekiem jāvalkā drošības nozīmītes, lai viņus būtu iespējams identificēt. Visiem Atea apmeklētājiem ir jāreģistrējas reģistratūrā, un viņiem ir jāizsniedz apmeklētāja nozīmīte, kas ir jātur redzamā vietā.

Visa sensitīvā informācija ir jānoņem no galdiem un droši jāglabā, kad tā netiek izmantota.

Mātesuzņēmums

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

Norvēģija

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

Zviedrija

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

Dānija

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

Somija

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

Lietuva

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

Loģistikas grupa

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

Grupas koplietotie pakalpojumi

Atea Global Services SIA
Mūkusalas iela 15
LV-1004 Rīga
+371 67359600
Org.nr. 50203101431
rigainfo@atea.com
ateaglobal.com

ATEA