TP2B THE PLACE TO BE

ATEA

INFORMATIONSSIKKERHED OG RISIKOSTYRING: REGLER FOR MEDARBEJDERE

Version 1.0 - udgivet august 2019

MEDDELELSE FRA SELSKABETS CEO

Hos Atea er det vores mission at “Build the Future with IT”.

Vi tror på, at informationsteknologi kombineret med viden og kreativitet kan forbedre produktiviteten og levestandarden generelt i samfundet. Vi hjælper erhvervslivet og offentlige instanser med at udvikle digitale løsninger, som gør dem i stand til at løse flere opgaver med større effektivitet og færre ressourcer.

Samtidig er vi bevidst om de risici, der er forbundet med teknologier, som bruges til at opbevare og behandle stadig flere informationer. Når virksomheder skal håndtere flere data og automatisere processer ved hjælp af sine it-systemer og netværk, er de udsat for store trusler som f.eks. datatyveri, identitetssvindel og driftsforstyrrelser som følge af cyber-angreb. Brud på datasikkerheden kan også resultere i, at en persons data tilgås uden vedkommendes samtykke og misbruges til at skade og krænke vedkommendes ret til privatliv.

Atea er en af de største leverandører af IT-teknologier i Norden og de baltiske lande og har et særligt ansvar for at sikre, at alle vores transaktioner overholder de strenge krav til informationssikkerheden. Atea udvikler, implementerer og leverer it-infrastrukturløsninger til de største og vigtigste organisationer i de lande, hvor vi opererer. Vi handler primært med nationale og lokale myndigheder, herunder sikkerhedsfølsomme kunder som f.eks. militæret og politiet. Vi tilbyder også forretningskritiske it-løsninger til nogle af de største virksomheder i disse lande.

Denne vejledning indeholder retningslinjer for håndtering af informationssikkerheden i Atea. Den giver et overblik over de vigtigste sikkerhedsrisici, databeskyttelsesregler og procedurer for databehandling, som påvirker alle i vores virksomhed. Det kræves, at alle medarbejdere med særligt ansvar for it-drift og systemadministration foretager målrettet og mere omfattende tests for overholdelse af vores informationssikkerhed og databeskyttelsesregler, afhængig af hvilken funktion de har.

Vejledningen er opdelt i fire afsnit, der hver især indeholder en sammenfatning til sidst i afsnittet. De fire afsnit indeholder detaljerede forklaringer, eftersom det er et kompliceret og vigtigt fokusområde. Det er især vigtigt, at du som medarbejder husker ”sammenfatningerne” til sidst i hvert afsnit og kan referere til resten af vejledningen, hvis det bliver nødvendigt.

Alle medarbejdere skal være bekendt med indholdet i denne vejledning. For at sikre at alle medarbejdere har forstået indholdet af vejledningen, har vi tilføjet 10 spørgsmål vedr. informationssikkerheden til gennemgang af adfærdskodeks´en (Code of Conduct), som er en obligatorisk test for alle Atea´s medarbejdere. Vi har lavet et online-modul til alle medarbejdere, som giver mulighed for at få mere at vide om Atea´s IT-sikkerhedspolitik og forberede sig på testen af viden om Adfærdskodeks´en (Code of Conduct).

Steinar Sønsteby
CEO

Atea er en stor virksomhed fordelt på ca. 90 kontorer, der opererer i 7 forskellige lande. Der er valgt en IT-sikkerhedsansvarlig for koncernen og en for hvert land, som bistår med at gennemføre/Implementere informationssikkerhedspolitikken i hele Atea.

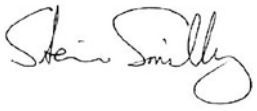
Hvis du har spørgsmål eller bemærkninger vedrørende Atea´s informationssikkerhed, bedes du rette henvendelse på følgende måde:

- Hvis du har mistanke om, at din pc kan være inficeret med malware eller har generelle spørgsmål vedrørende it-sikkerhed, er du velkommen til at kontakte Atea Servicedesk
- For at anmelde en mistænkelig e-mail, forsøg på svindel eller andet, der kan udgøre en sikkerhedsrisiko for Atea, bedes du rette henvendelse til Atea Servicedesk.
- For at anmelde mistanke om brud (uautoriseret videregivelse) på datasikkerheden i forhold til person- eller virksomhedsoplysninger via informationssystemer og dokumenter, bedes du rette henvendelse til DPO (Data Protection Officer) e-mail: dpo@atea.dk eller til it-sikkerhedschefen i det land, hvor du arbejder. Du kan også sende en e-mail direkte til infosec@atea.com.

Hvis du ønsker at tale direkte med den øverste it-sikkerhedsansvarlige (CISO) for hele Atea-koncernen eller it-sikkerhedschefen for dit land eller serviceenhed, finder du deres kontaktoplysninger på Atea´s hjemmeside under Compliance: atea.com/trust. Alle mails, der sendes til infosec@atea.com bliver videresendt til Atea-koncernens øverste it-sikkerhedsansvarlige.

Vi modtager gerne dine spørgsmål og feedback og garantere, at der ikke vil ske repressalier mod personer, der anmelder mistænkelige forhold. Hvis du foretrækker at foretage en anonym anmeldelse, kan du sende din anmeldelse til vores Whistleblower Hotline. Du finder link til whistleblower-ordningen på Atea´s hjemmeside under Compliance: atea.com/trust. Anmeldelser, der foretages via vores whistleblower-ordning, videresendes til et advokatfirma, der sammenfatter og indberetter din mistanke om ureglementerede forhold til rette vedkommende i Atea´s organisation.

Det er meget vigtigt for vores forretning, at vi stiller strenge krav til datasikkerheden, så vi er i stand til at samarbejde med vores kunder og partnere om de største it-udfordringer i vores branche. Tak fordi du efterlever Atea´s informationssikkerhedsregler/politikker og for at gøre Atea til "The Place to Be".



Sammenfatning:

Det er vigtigt for os, at alle medarbejdere overholder de strenge krav til datasikkerheden.

Der er valgt en it-sikkerhedsansvarlig for koncernen og en for hvert land, som bistår med at gennemføre informationssikkerhedspolitikken i hele Atea. Du finder kontaktoplysninger til it-sikkerhedscheferne på Atea´s hjemmeside under Compliance: atea.com/trust.

Hvis du har spørgsmål eller bemærkninger vedrørende Atea´s informationssikkerhed, bedes du rette henvendelse på følgende måde:

- Hvis du har mistanke om, at din pc kan være inficeret med malware eller har generelle spørgsmål vedrørende it-sikkerhed, er du velkommen til at kontakte Atea Servicedesk
- For at anmelde en mistænkelig e-mail, forsøg på svindel eller andet, der kan udgøre en sikkerhedsrisiko for Atea, bedes du rette henvendelse til Atea Servicedesk.
- For at anmelde mistanke om brud (uautoriseret videregivelse) på datasikkerheden i forhold til person- eller virksomhedsoplysninger via informationssystemer og dokumenter, bedes du rette henvendelse til DPO´en (Data Protection Officer) eller it-sikkerhedschefen i det land, hvor du arbejder.
- Du kan også sende en e-mail til infosec@atea.com, som videresender til Atea-koncernens øverste it-sikkerhedsansvarlige

Indhold

1. Informationssikkerhed – overblik og risikostyring 5
2. Databeskyttelse – overblik og risikostyring 8
3. Atea's databeskyttelsesregler 10
4. Beskyttelse af IT-infrastruktur – obligatorisk praksis for alle medarbejdere 15

1. INFORMATIONSSIKKERHED – OVERBLIK OG RISIKOSTYRING

Information er afgørende for, at en virksomhed kan fungere optimalt. Et system til varetagelse af it-sikkerheden (ISMS) består af en række politikker, procedurer, værktøjer og aktiviteter, som en virksomhed bruger til at beskytte sine oplysninger mod uautoriseret adgang og misbrug.

Udarbejdelse af et sådan system kræver, at virksomheden identificerer de oplysninger, den er i besiddelse af. Dette omfatter alle oplysninger, som virksomheden behandler i enhver form, dvs. digitalt, i papirform eller mundtligt. I Atea er disse oplysninger f.eks. til intern brug eller omfatter eksterne oplysninger, som Atea administrerer og behandler som en service for vores kunder.

Formålet med et system til varetagelse af it-sikkerheden, er at beskytte og behandle oplysninger fortroligt og sikkert samt stille informationer til rådighed.

- **Ved fortrolighed** forstås, at oplysningerne kun videregives til autoriserede personer.
- **Ved integritet** forstås, at oplysningerne opbevares korrekt og er fuldstændige.
- **Ved tilgængelighed** forstås, at autoriserede brugere kan tilgå og anvende oplysninger, når det er nødvendigt.

For at opfylde disse formål skal virksomheden foretage en risikovurdering for at identificere, hvorvidt informationerne er eksponeret for et eventuelt brud på informationssikkerheden. Derefter kan der udformes et system til varetagelse af it-sikkerheden, som kan håndtere, kontrollere mimere disse risici på en effektiv måde uden unødige omkostninger eller tab af produktivitet.

Atea´s risikovurderinger

Nedenstående overordnet informationssikkerhedsrisici er identificeret og har højeste prioritet for Atea:

1. Fysisk tab:

Informationer opbevares på fysiske enheder, som kan gå tabt, blive stjålet eller beskadiget. Adgangskontrol, kryptering og sikkerhedskopiering af data er vigtigt for at begrænse mulige risici i forbindelse med fysiske enheder, som f.eks. pc'er, telefoner, servere og storage. Datacentre skal beskyttes mod miljøfarer, og bl.a. herunder svingende temperaturer og brand.

2. Identitetssvindel:

Atea er konstant udsat for forsøg på svindel, som bl.a. benytter falske identiteter eller svindler for at udnytte medarbejderens tillid. Formålet med denne form for forsøg på svindel er som regel at stjæle fra Atea, og opnå en økonomisk gevinst eller med henblik på at opnå uautoriseret adgang til Atea´s systemer og netværk.

Én af de former for identitetssvindel, som Atea oplever, er brug af falske eller stjålne kundeoplysninger til at bestille it-udstyr, navnlig via Atea´s webshop. Ud over adgangskontrol på webshoppen bruger Atea forretningsprocedurer med henblik på at screene nye kundeprofiler og identificere usædvanlig kundeaktivitet på eksisterende konti for at mindske risikoen for svigagtige kundetransaktioner.

En anden hyppig form for identitetssvindel (også kaldet "phishing"), som Atea oplever, er når en af Atea´s medarbejdere får tilsendt en e-mail direkte fra svindleren. E-mailen kommer tilsyneladende fra en pålidelig kilde, ofte ved hjælp af en falsk identitet som f.eks. en anden Atea-medarbejder, en forretningsforbindelse eller en leverandør, som f.eks. en teknologivirksomhed eller en bank. E-mailen forsøger at narre Atea-medarbejderen til at svare, f.eks. i form af at foretage pengeoverførsler, indtaste login/adgangskode eller andre følsomme oplysninger, eller til at klikke på et link eller en vedhæftet fil, der downloader ondsindede programmer (også kaldet "malware") på brugerens pc eller mobil.

Mailen, den vedhæftede fil eller linket ser ud til at være helt uskyldig - udgiver sig f.eks. for at være en mail fra en kollega, et tilbud/faktura fra en leverandør eller en meddelelse fra en Cloud-konto såsom OneDrive. Derfor skal Atea´s medarbejdere være meget på vagt overfor risikoen for svindel i e-mails eller anden kommunikation, selvom det tilsyneladende kommer fra en pålidelig kilde.

Atea´s medarbejdere bør aldrig åbne vedhæftede filer eller link, hvis der er tvivl om en mails eller meddelelses pålidelighed. Hvis en med-

arbejder er i tvivl om en e-mails pålidelighed, eller hvis vedkommende ved et uheld har reageret på et potentielt forsøg på svindel ved at åbne et mistænkeligt link eller en vedhæftet fil, skal Atea Servicedesk straks kontaktes og forholdet anmeldes.

Selvom e-mail er den mest almindelige metode til phishing-angreb på arbejdspladsen, bør Atea´s medarbejdere også være opmærksom på andre former for svigagtig kommunikation, herunder telefoniske henvendelser eller invitationer via de sociale medier.

3. Tyveri af forretningshemmeligheder:

Hvis uautoriserede personer får adgang til Atea´s informationssystemer, kan de forsøge at stjæle fortrolige oplysninger, der er følsomme for Atea´s forretning. Det kan f.eks. være fortrolige virksomhedsoplysninger, såsom kunde- og leverandøroplysninger og forretningsbetingelser. Det kan også være immaterielle rettigheder som f.eks. forretningskoncepter, produkter eller design og internt udviklet software, metoder og værktøjer.

Medarbejdere med adgang til vigtige systemer kan forsøge at tilegne sig forretnings-hemmeligheder fra Atea, særligt hvis disse medarbejdere påtænker at forlade Atea. For at mindske risikoen må der kun gives adgang til oplysninger for medarbejdere på "need to know" basis. Adgangen til systemet skal løbende screenes for at sikre, at "need to know" princippet opdateres, og at brugerens adgangsrettigheder annulleres, når de ikke længere er nødvendige.

Ud over adgangskontrol benytter Atea Security Information and Event Management (SIEM) -værktøjer til at analysere log-oplysninger og undersøge, hvilke transaktioner der er foretaget på virksomhedens systemer.

4. Driftsforstyrrelser:

Atea´s forretningsaktiviteter er afhængig af it-systemer. I tilfælde af overtrædelse af kontrolforanstaltninger, eller hvis systemer misbruges, kan der potentielt være sket læk af medarbejderes eller forretningspartneres personlige oplysninger. Oplysninger, der er nødvendige for Atea´s forretningsdrift, kan være blevet manipuleret eller slettet. Endvidere kan virksomhedstransaktioner tilgås og godkendes af uvedkommende i strid med Atea´s kontrolforanstaltninger. Alt dette griber forstyrrende ind på driften af Atea´s forretning.

Atea er også udsat for driftsforstyrrelser som følge af avancerede hackerangreb, der forårsager nedbrud på vigtige it-systemer eller netværk. Systemer kan være inficeret med malware, der forhindrer brugerne i at få adgang til vigtige funktioner eller fra ind- og udlæsning af filer, medmindre der betales en løsesum ("ransomware"). Netværk eller ´servere kan blive oversvømmet med trafik eller anmodninger, så de ikke længere kan håndtere legitime transaktioner (også kaldet denial of service eller DoS-angreb). Disse angreb kan være rettet mod enten Atea eller de kunder, som Atea er administrator for.

5. Kontraktforhold:

Atea har indgået fortrolighedsaftaler med flere kunder, leverandører og samarbejdspartnere. Atea har også indgået serviceaftaler og databehandlingsaftaler med kunder, der benytter Atea´s it-tjenester og support.

Et brud på it-sikkerheden hos Atea kan medføre brud på tavshedspligt, serviceniveau og databehandlingsaftaler med kunder og andre samarbejdspartnere. Dette kan resultere i sagsanlæg mod Atea med krav om erstatning som følge af overtrædelse af kontrakter. Udover direkte skader kan et brud på it-sikkerheden forårsage varig skade på Atea´s forretningsforbindelser med kunder og partnere.

Selv i situationer, hvor Atea ikke har indgået en specifik aftale, kan Atea blive mødt med retskrav fra virksomheder eller enkeltpersoner i tilfælde af, at deres data bliver stjålet eller misbrugt, såfremt Atea ikke har udvist fornøden omhu og agtpågivenhed med hensyn til behandling af oplysningerne.

6. Lovgivningsmæssige sanktioner:

Som børsnoteret selskab på Oslo Børs er Atea forpligtet til at følge strenge lovkrav i forbindelse

med behandling af oplysninger, som ikke er kendt i markedet, og som kan påvirke Atea´s aktiekurs (også kaldet "prisfølsomme oplysninger"). Det kan f.eks. være oplysninger om nye store kontrakter eller økonomiske resultater, som endnu ikke er blevet offentliggjort.

Atea skal behandle prisfølsomme oplysninger fortroligt for at sikre, at disse oplysninger ikke videregives til andre end et begrænset antal registrerede insidere på "need to know" basis. Medarbejdere, der er i besiddelse af prisfølsomme oplysninger, skal registreres af virksomheden og er underlagt særlige krav til fortrolighed og restriktioner for handel med Atea-aktier. Overtrædelse af disse lovkrav er strafbart og kan medføre bødestraf i henhold til den norske lov om værdipapirhandel.

Atea er også underlagt lovgivningsmæssige sanktioner i tilfælde af brud på datasikkerheden i forhold til personoplysninger i henhold til EU's generelle forordning om databeskyttelse (GDPR). Eftersom GDPR-kravene er ret omfattende, vil dette emne blive behandlet særskilt i næste afsnit under databeskyttelse.

Sammenfatning:

Alle medarbejdere skal være meget påpasselige, når de behandler oplysninger og benytter it-systemer for at undgå brud på sikkerheden.

It-udstyr kan gå tabt, blive stjålet eller beskadiget. Adgangskontrol, kryptering og sikkerhedskopiering af data er derfor vigtigt for at begrænse eventuelle brud på informationssikkerheden.

Atea er konstant udsat for forsøg på svindel begået af svindlere, som benytter falske identiteter eller svindler for at udnytte medarbejderens tillid. Vær opmærksom på, at alle e-mails eller anden kommunikation, du modtager, kan være forsøg på svindel, selvom det tilsyneladende kommer fra en pålidelig kilde (som f.eks. en e-mail fra en af Atea´s chefer, en kunde, en leverandør eller en social mediekonto).

Vær på vagt over for usædvanlig kommunikation eller aktivitet, som du støder på. Hvis du har mistanke om, at du er i farezonen for svindel via e-mail eller anden meddelelse, bedes du kontakte Atea Servicedesk omkring forholdet.

Undlad at reagere på mistænkelig kommunikation, f.eks. ved at åbne vedhæftede filer i mails og eksterne link eller ved at behandle ordrer og betalinger.

Adgang til oplysninger må kun gives til medarbejdere på "need to know" basis for at mindske risikoen for tyveri eller misbrug. Adgangen til systemet skal løbende screenes for at sikre, at brugerens adgangsrettigheder annulleres, når de ikke længere er nødvendige.

Brud på informationssikkerheden kan medføre alvorlig skade for Atea i form af driftsforstyrrelser, brud på Atea´s kontraktlige forpligtelser overfor kunder og samarbejdspartnere, lovgivningsmæssige sanktioner samt skade på Atea´s omdømme og forretningsforbindelser.

2. DATABESKYTTELSE – OVERBLIK OG RISIKOSTYRING

Databeskyttelse indebærer en persons kontrol over egne oplysninger - navnlig muligheden for at bestemme hvornår og hvordan personoplysninger indsamles, deles og bruges. Ved personoplysninger forstås enhver form for oplysninger, der kan føres tilbage til en specifik og identificerbar person.

Datasikkerhed er afhængig af informations-sikkerhed, dvs. hvordan data beskyttes mod uautoriseret adgang og misbrug. Men datasikkerhed omfatter mere end informations-sikkerhed, idet det også dækker beskyttelse af den enkeltes ret til sine personoplysninger. Navnlig hvordan en virksomhed giver den enkelte mulighed for kontrol over sine personoplysninger, når virksomheden indsamler og behandler oplysninger vedrørende den pågældende person.

Vi mener, at databeskyttelse er en grundlæggende menneskeret, og vi lægger vægt på at behandle personoplysninger på en måde, der fuldt ud respekterer denne ret. Atea er underlagt strenge lovkrav i forbindelse med behandling af personoplysninger i henhold til databeskyttelsesforordningen (også kaldet EU's generelle forordning om databeskyttelse).

GDPR-kravene, der gælder for Atea, kan sammenfattes således:

Krav ved indsamling af personoplysninger
Atea må alene behandle (f.eks. indsamle, opbevare og bruge) personoplysninger, når de har en legitim interesse, og når den pågældende person har givet sit samtykke eller er blevet orienteret om, at vedkommendes personoplysninger bliver behandlet. Oplysningerne i denne orientering eller samtykke er beskrevet i næste afsnit.

Personers ret til kontrol over deres personoplysninger
Atea skal efterkomme en persons anmodning om kontrol over brug af vedkommendes personoplysninger i overensstemmelse med ret til beskyttelse af privatlivets fred i henhold til GDPR. I henhold til databeskyttelsesforordningen har fysiske personer ret til indsigt i deres personoplysninger, som Atea er i besiddelse af. Fysiske personer har også ret til berigtigelse af urigtige personoplysninger, til at få deres personoplysninger slettet eller til at begrænse behandlingen af deres personoplysninger.

Dokumentation for behandling
Atea skal dokumentere omfanget af deres databehandlingsaktiviteter vedrørende personoplysninger. Det omfatter en beskrivelse af, hvilke typer personoplysninger der behandles, samt for hvilke kategorier af personer. Det omfatter desuden en beskrivelse af, hvilke tekniske og organisatoriske foranstaltninger der er truffet for at forebygge og minimere følgerne af brud på datasikkerheden i forbindelse med Atea´s databehandlingsaktiviteter (også kaldet "privacy by design" eller indbygget databeskyttelse).

Databehandlingsaftaler med kunder/leverandører
Når Atea leverer databehandlingstjenester til sine kunder (f.eks. når Atea håndterer datainfrastruktur og applikationer for kunderne, enten hos kunden eller fra sine egne datacentre), skal der være indgået en gyldig databehandlingsaftale (DBA) med kunden, som stemmer overens med GDPR-kravene.

Når Atea behandler personoplysninger gennem en underleverandør eller en leverandør (f.eks. når vi benytter softwareprogrammer, der driftes i en leverandørs datacenter, såsom Cloud-tjenester), skal der ligeledes være indgået en gyldig databehandlingsaftale i overensstemmelse med GDPR med virksomheden, der administrerer programmet og behandlingen af personoplysninger på vegne af Atea. Oplysninger, der behandles uden for EU/EØS, skal være i et land eller inden for de rammer, som de offentlige myndigheder har anerkendt som værende fornødne garantier for databeskyttelse.

Krav i tilfælde af brud på datasikkerheden
I tilfælde af brud på persondatasikkerheden, som kan være til skade for en person, skal Atea underrette tilsynsmyndigheden i det land, hvor bruddet er sket inden for 72 timer efter at have fået kendskab dertil. Denne underretning omfatter en beskrivelse af bruddets karakter, en oversigt over

de berørte registrerede og fortegnelser, bruddets forventede konsekvenser, samt hvilke foranstaltninger der er truffet.

I henhold til databeskyttelsesforordningen kan tilsynsmyndigheden i det enkelte land pålægge en virksomhed sanktioner i tilfælde af brud på forordningen. Sanktionens størrelse afhænger af bruddets karakter, omfanget af krænkelser af rettigheder vedrørende personoplysninger, samt hvilke foranstaltninger virksomheden har truffet for at forebygge og afhjælpe krænkelsen. Sanktionens størrelse i tilfælde af brud på forordningen kan ikke overstige 4 % af de samlede årlige indtægter eller 20 mio. euro, afhængigt af hvad der er højest.

På grund af GDPR-kravene er det yderst vigtigt, at Atea dokumenterer alle processer vedrørende personoplysninger og identificerer alle interne systemer og aftaler, der omhandler behandling af personoplysninger. Disse oplysninger skal være tilgængelige for it-sikkerhedschefen for hvert land for at bekræfte, at fornødne foranstaltninger for at beskytte datasikkerheden er truffet. Kontaktoplysninger til det enkelte lands og koncernens øverste it-sikkerhedsansvarlige kan findes på Atea´s hjemmeside under Compliance.

Sammenfatning:

Databeskyttelse indebærer en persons kontrol over egne oplysninger - navnlig muligheden for at bestemme hvornår og hvordan personoplysninger indsamles, deles og bruges. Ved personoplysninger forstås enhver form for oplysninger, der kan føres tilbage til en specifik og identificerbar person.

Atea er underlagt strenge lovkrav i forbindelse med behandling af personoplysninger i henhold til databeskyttelsesforordningen (også kaldet EU's generelle forordning om databeskyttelse).

I henhold til databeskyttelsesforordningen:
må Atea alene behandle (f.eks. indsamle, opbevare og bruge) personoplysninger, når de har en legitim interesse, og når den pågældende person har givet sit samtykke eller er blevet orienteret om, at vedkommendes personoplysninger bliver behandlet.

skal Atea efterkomme en persons anmodning om kontrol over brug af vedkommendes personoplysninger i overensstemmelse med ret til beskyttelse af privatlivets fred i henhold til GDPR.

skal Atea dokumentere omfanget af sine databehandlingsaktiviteter vedrørende personoplysninger, herunder hvilke foranstaltninger, der er truffet for at forebygge og mindske følgerne af et brud på datasikkerheden. Det kræver, at Atea dokumenterer alle processer vedrørende personoplysninger og identificerer alle interne systemer og aftaler, der omhandler behandling af personoplysninger.

Atea skal have indgået en gyldig databehandlingsaftale med alle de kunder, som de leverer databehandlingstjenester til (f.eks. håndtering af datainfrastruktur og applikationer, enten hos kunden eller fra sine egne datacentre).

Atea skal også have indgået en gyldig databehandlingsaftale med alle underleverandører eller leverandører, som behandler personoplysninger på vegne af Atea (f.eks. levering af softwareprogrammer og dataopbevaring, der driftes i leverandørens datacenter, som f.eks. Cloudtjenester).

I tilfælde af brud på persondatasikkerheden, som kan medføre risiko for at skade for en fysisk person, skal Atea underrette tilsynsmyndigheden i det land, hvor bruddet er sket inden for 72 timer efter at have fået kendskab dertil.

3. ATEA´S DATABESKYTTELSESREGLER

Atea´s medarbejdere skal til enhver tid overholde virksomhedens databeskyttelsesregler i forbindelse med indsamling, behandling og videregivelse af data. Alle Atea´s ledere skal sikre, at forretningsprocesser inden for deres ansvarsområde følger Atea´s databeskyttelsesregler, og at deres medarbejdere agerer i henhold til disse processer.

Alle Atea´s ledere vil blive tilknyttet en Databeskyttelsesadministrator, som bliver ansvarlig for en specifik funktion i den pågældendes land (eller serviceenhed). Det vil være databeskyttelsesadministratorens opgave at påse, at alle forretningsprocesser inden for vedkommendes funktion overholder Atea´s databeskyttelsesregler. Disse funktioner omfatter: Salg/Marketing, HR, Finans, Konsulenttjenester, AMS, Logistik og IT.

Databeskyttelsesadministratoren for hver funktion vil referere til it-sikkerhedschefen for det pågældende land (eller serviceenhed). It-sikkerhedschefen for hvert land har det overordnede ansvar for gennemførelse af databeskyttelsesreglerne i det pågældende land og refererer til den øverste it-sikkerhedsansvarlige for hele koncernen.

Kontaktoplysninger til alle nøglemedarbejdere i it-sikkerhedsafdelingen i dit land kan du finde på Atea´s hjemmeside under Compliance: atea.com/trust. En oversigt over it-sikkerhedsorganisation fremgår desuden af tillægget til denne vejledning.

Atea´s databeskyttelsesregler omfatter:

- Systemregistrering
- Dataklassificering
- Administration af personoplysninger
- Kundeaftaler

Oversigt over databeskyttelsesregler:

Systemregistrering
Før Atea´s medarbejdere påbegynder indsamling, behandling eller videregivelse af oplysninger, skal de bekræfte, at alle informationssystemer til opbevaring eller behandling af oplysningerne er godkendt af det pågældende lands it-sikkerhedschef. Dette omfatter også Cloud-tjenester, der købes på abonnementsbasis og administreres eksternt.

It-sikkerhedschefen eller systemejeren foretager en analyse af it-sikkerheden og informationssystemets standarder i forhold til beskyttelse af privatlivets fred (DPIA) forud for registrering af systemet, der skal godkendes til brug hos Atea.

Analysen bygger på en tjekliste af it-sikkerheden og databeskyttelsesregler hos Atea, som udfyldes sammen med Atea-koncernens øverste it-sikkerhedsansvarlige.

Den it-sikkerhedsansvarlige eller systemejeren overvejer også, hvilken type oplysninger og om følsomme oplysninger skal opbevares i systemet, i forbindelse med vurderingen af, om systemet opfylder Atea´s informationssikkerhedskrav. Som led i analysen vedtages regler for sletning af personoplysninger i systemet, når de ikke længere er nødvendige for Atea (også kaldet "dataminimering").

Hvis informationssystemet administreres eksternt og indeholder personoplysninger - f.eks. et Cloud-baseret HR-system - skal Atea have indgået en skriftlig databehandlingsaftale med tjenesteudbyderen for at opfylde kravene i GDPR. Du finder en standard databehandlingsaftale for Cloud-tjenesteudbydere på dit lands intranet under Global Information Security. DPO´en eller It-sikkerhedschefen i hvert land kan besvare spørgsmål vedrørende databehandlingsaftalen.

Atea´s medarbejdere må ikke opbevare eller behandle virksomhedsoplysninger i "it-undersystemer", der ikke er registreret af deres lands DPO. Atea´s medarbejdere må ikke foretage væsentlige ændringer i databehandlingssystemer og -processer, uden at have underrettet DPO´en eller it-sikkerhedschefen, således at der kan foretages en ny vurdering af it-sikkerheden.

Systemejeren skal sikre, at systemet anvendes i overensstemmelse med Atea´s databeskyttelsesregler. Systemejeren skal navnligt sikre, at adgangsrettigheder til systemet er begrænset til dem, der "need to know", og at rettighederne annulleres, så snart de ikke længere er nødvendige. Systemejeren skal desuden sikre, at personoplysninger, der er opbevaret i systemet, bliver slettet, når de ikke længere er nødvendige for Atea, i overensstemmelse med den aftalte dataminimeringspolitik, når systemet godkendes til brug.

Dataklassificering
Når et system er godkendt til brug i Atea, dokumenteres hvilken type oplysninger og om

følsomme oplysninger opbevares i systemet for at sikre, at fornødne databeskyttelsesregler er på plads.

Atea´s medarbejdere vil dog i mange tilfælde skulle behandle og videregive oplysninger uden for et godkendt it-system. Det omfatter oplysninger, der behandles via trykte dokumenter, e-mail eller fildeling (f.eks. Microsoft Word/Excel/Powerpoint-filer).

For at sikre at oplysninger, der opbevares uden for et godkendt it-system administreres på det fornødne sikkerhedsniveau, skal Atea´s medarbejdere sørge for at mærke filer, dokumenter eller e-mails, der indeholder oplysninger i forhold til, hvor følsomme oplysningerne er, således at det er nemt for modtageren af oplysningerne at se det. Denne mærkning skal følge Atea´s regler for klassificering af data.

Atea´s regler for dataklassificering består af fem niveauer, som opdeler de opbevarede oplysninger i e-mailen eller filen efter, hvor følsomme de er. Klassificeringsreglerne er integreret i Atea´s versioner af Microsoft Outlook og Word/Excel/Powerpoint. Atea´s medarbejdere kan automatisk mærke en e-mail, et dokument eller en fil med korrekt dataklassificeringsmærkning ved at klikke på en knap øverst i disse programmer.

De fem niveauer er som følger:

1. Private (Non-business): Privat e-mailkorrespondance og dokumenter, som ikke vedrører Atea.

2. Offentlige (Public): Oplysninger om Atea, som kan offentliggøres.

3. Interne (Internal): Oplysninger, der frit kan videregives internt i Atea, herunder til de respektive Atea selskaber i forskellige lande, samt 3. parts leverandører underlagt kontrakt. Disse er ikke beregnet til videregivelse uden for Atea eller til aftaleparter.

4. Fortrolige (Confidential): Oplysninger, som ikke må deles uden ejeren af oplysningernes tilladelse. Dette omfatter personoplysninger, der skal mærkes særskilt. Mærkning af personoplysninger kan tilføjes via rullemenuen under fanen Fortrolige.

5. Strengt fortrolige (Strictly confidential): Oplysninger, som kan få betydelige negative konsekvenser for Atea, hvis de videregives uden tilladelse. Disse oplysninger skal opbevares i krypteret format og må ikke videregives uden tilladelse fra ejeren af oplysningerne. Sådanne oplysninger omfatter:

- Personfølsomme oplysninger: I henhold til databeskyttelsesforordningen skal der træffes ekstra sikkerhedsforanstaltninger ved behandling af særlige kategorier af personoplysninger. Dette omfatter oplysninger om: etnisk oprindelse, politisk anskuelse, religion, fagforeningstilslutning og genetiske eller biometriske data. Følsomme personoplysninger skal mærkes særskilt. Mærkningen kan tilføjes via rullemenuen under fanen Strengt fortrolige.

- Virksomhedsfølsomme oplysninger: Dette omfatter virksomhedsoplysninger som f.eks. vigtige kunde- og leverandøroplysninger samt forretningsbetingelser. Det omfatter også oplysninger, som er belagt med tavshedspligt eller omfattet af en fortrolighedsaftale med en kunde eller samarbejdspartner. Endelig kan det omfatte meget følsomme immaterielle rettigheder som f.eks. forretningskoncepter og internt udviklet software, metoder og værktøjer.

- Følsomme prisoplysninger: Følsomme prisoplysninger er en særlig form for fortrolige oplysninger, som kan påvirke Atea´s aktiekurs. Dette kan blandt andet omfatte væsentlige finansielle oplysninger, som endnu ikke er blevet offentliggjort, eller status for fortrolige forhandlinger vedrørende en meget stor kundekontrakt eller aftale.

- Atea´s økonomidirektør skal underrettes om samtlige medarbejdere, der er i besiddelse af følsomme prisoplysninger: Disse medarbejdere vil blive registreret i Computershare Insider Management System (CIMS), som Atea benytter. Yderligere oplysninger om procedurer vedrørende regler for følsomme prisoplysninger fremgår af vores Adfærdskodeks.

En komplet beskrivelse af Atea´s dataklassificeringsregler og procedurer for mærkning og kryptering af dokumenter og e-mailkorrespondance fremgår af hjemmesiden under Global Information Security på dit lands intranet. (https://atea.sharepoint.com/sites/com-gdpr/Pages/GDPR-for-Atea-employees.aspx)

Administration af personoplysninger

I henhold til databeskyttelsesforordningen har Atea særlige retlige forpligtelser med hensyn til behandling af personoplysninger – oplysninger, der kan føres tilbage til en specifik og identificerbar person. Disse retlige forpligtelser betyder, at Atea skal dokumentere, at de har truffet de fornødne tekniske og organisatoriske foranstaltninger for at efterkomme kravene i databeskyttelsesforordningen. Denne dokumentation af procedurer skal være tilgængelig på anmodning fra de offentlige myndigheder.

Før Atea kan indsamle personoplysninger, skal forretningsprocessen, hvorigennem personoplysningerne skal behandles, være fuldt dokumenteret og vurderet af it-sikkerhedschefen. Databeskyttelsesadministratoren for hver funktion skal sikre, at alle processer til behandling af personoplysninger inden for deres funktionsområde er dokumenteret og ajourførte i overensstemmelse med GDPR.

Dokumentationen skal godtgøre, at Atea har truffet de fornødne tekniske og organisatoriske foranstaltninger for at efterkomme den enkeltes ret til sine personoplysninger med henblik på at forebygge og minimere risikoen for brud på datasikkerheden og reagere i tilfælde af brud på persondatasikkerheden. Metoderne til indsamling af personoplysninger skal også indeholde en procedure for dataminimering, dvs. sletning af personoplysninger når de ikke længere er nødvendige for Atea.

Når vi indsamler personoplysninger, skal den enkelte person underrettes eller der skal indhentes samtykke til at vedkommendes personoplysninger indsamles og bruges. Ved underretning eller indhentning af samtykke hos en person; skal Atea i henhold til databeskyttelsesforordningen oplyse følgende:

1. Hvilke kategorier af personoplysninger der indsamles og behandles
2. Formålet med og retsgrundlaget for databehandlingen
3. Modtagerne af personoplysningerne, eller kategorier af modtagere
4. Tidsrum, hvor oplysningerne vil blive brugt, eller hvilke kriterier der fastlægger dette tidsrum
5. Den enkeltes ret til sine personoplysninger - herunder ret til at tilbagetrække samtykke og ret til indsigt, sletning og berigtigelse
6. Den enkeltes ret til at indgive en klage til tilsynsmyndigheden.
7. I givet fald underretning om, at oplysningerne vil blive overført til et andet land, samt bekræftelse af at enhver behandling af oplysninger i et andet land vil ske i henhold til bestemmelserne i databeskyttelsesforordningen om fornøden databeskyttelse
8. Hvis personfølsomme data bliver indsamlet, skal Atea anmode om og indhente udtrykkeligt samtykke fra personen, hvis personoplysninger behandles.
9. Atea landets DPO skal kontaktes hvis en henvendelse kommer fra en person (Data Subject)

Du finder en standard privatlivsmeddelelse til indsamling af personoplysninger på hjemmesiden under Global Information Security på dit lands intranet.

Atea har særlige forpligtelser i henhold til databeskyttelsesforordningen i tilfælde af brud på datasikkerheden i forbindelse med personoplysninger. Brud på datasikkerheden er et brud på informationssikkerheden, der medfører, at uautoriserede personer får adgang til data, eller resulterer i ulovlige eller utilsigtede tab af data.

I tilfælde af brud på datasikkerheden skal Atea´s medarbejdere straks underrette it-sikkerhedschefen for deres land eller DPO´en. It-sikkerhedschefen vil sammen med DPO´en samt Atea´s it-sikkerhedsorganisation undersøge databruddet og træffe nødvendige afhjælpende foranstaltninger for at rapportere og begrænse de skader, som bruddet på datasikkerheden har forvoldt.

Hvis bruddet på datasikkerheden vedrører personoplysninger og medfører risiko for at skade en fysisk person, skal Atea underrette tilsynsmyndighederne i det land, hvor bruddet konstateret er sket inden for 72 timer efter at have fået kendskab dertil. Denne underretning omfatter en beskrivelse af bruddets karakter, en oversigt over de berørte registrerede og fortegnelser, bruddets forventede konsekvenser, samt hvilke foranstaltninger der er truffet.

Fysiske personer, for hvem der er sket brud på persondatasikkerheden, skal også underrettes direkte, hvis der er stor risiko for at skade vedkommende. En offentlig meddelelse kan være tilstrækkeligt, hvis underretning af enkeltpersoner ikke er muligt.

Kundeaftaler

Atea håndterer datainfrastruktur og applikationer for mange kunder, enten hos kunden eller fra sine egne datacentre. I disse tilfælde er Atea kontraktligt ansvarlig for behandlingen af kundens data og har en retlig forpligtelse i henhold til databeskyttelsesforordningen til at sikre tilstedeværelse af de fornødne garantier i forbindelse med rettigheder vedrørende personoplysninger tilhørende alle fysiske personer, hvis personoplysninger er medtaget i kundens data.

For at opfylde kravene i GDPR skal Atea have indgået en databehandlingsaftale med sine kunder, når kundens datainfrastruktur og applikationer administreres. Databehandlingsaftalen skal dokumentere omfanget, karakteren og varigheden af de databehandlingsaktiviteter, som Atea varetager efter instruks fra kunden. Denne dokumentation skal også omfatte en redegørelse for, hvilke typer personoplysninger Atea behandler på vegne af kunden, samt hvilke kategorier af personer der får deres personoplysninger behandlet.

Databehandlingsaftalen skal indeholde følgende bekræftelse fra Atea i henhold til databeskyttelsesforordningen:

1. Atea behandler kun personoplysninger efter dokumenterede instrukser fra sin kunde og overholder databeskyttelseslovgivningen
2. Atea´s medarbejdere, der behandler personoplysninger for kunden, har forpligtet sig til fortrolighed. Atea kan ikke udpege underleverandører til at behandle personoplysninger for kunden uden kundens tilladelse.
3. Atea har truffet de fornødne tekniske og organisatoriske foranstaltninger for at tilvejebringe et sikkerhedsniveau, der er aftalt med kunden i forhold til risikoen ved de oplysninger, der behandles.
4. Atea har truffet tilstrækkelige foranstaltninger til at opfylde sine retlige forpligtelser i forhold til personers ret til kontrol over behandlingen af deres oplysninger, som beskrevet i databeskyttelsesforordningen.
5. Atea vil give kunden de oplysninger, der er nødvendige for at påvise opfyldelse af deres databeskyttelsesforpligtelser i henhold til databeskyttelsesforordningen, og deltage i kundens overholdelseskontroller på anmodning
6. Atea vil underrette kunden om eventuelle brud på persondatasikkerheden uden unødig forsinkelse
7. Atea vil slette eller returnere alle personoplysninger til kunden ved serviceaftalens udløb

Hvis Atea benytter eksterne underleverandører for at opfylde sine databehandlingsforpligtelser over for kunden (f.eks. tredjeparts Cloud-tjenester, konsulenter eller infrastrukturudbydere) skal Atea have indgået en databehandlingsaftale med disse underleverandører, hvori underleverandører giver en lignende bekræftelse på ovenstående.

Atea har en standard databehandlingsaftale, som anbefales til brug for alle kunder og underleverandører. Databehandlingsaftalen finder du på hjemmesiden under Global Information Security på dit lands intranet. It-sikkerhedschefen i hvert land kan besvare spørgsmål vedrørende databehandlingsaftalen og kan hjælpe med at indhente en skriftlig databehandlingsaftale fra kunden eller underleverandøren.

I tilfælde af brud på persondatasikkerheden i forhold til kundens data skal Atea underrette kunden uden forsinkelse, når Atea er blevet bekendt med bruddet på datasikkerheden. Atea skal derefter bistå kunden og træffe rimelige foranstaltninger for at sikre, at kunden kan leve op til sine forpligtelser om at rapportere bruddet på datasikkerheden, som foreskrevet i databeskyttelsesforordningen, og træffe afhjælpende foranstaltninger for at begrænse de skader, som bruddet har forvoldt.

Sammenfatning:

Systemregistrering
Alle it-systemer, der anvendes i Atea, skal registreres hos den øverste it-sikkerhedschef i det land eller forretningsenheden, hvor systemet er i brug. Dette omfatter Cloud-tjenester, der købes på abonnementsbasis og administreres eksternt.

It-sikkerhedschefen vil gennemgå it-systemet for at bekræfte, at det opfylder Atea´s it-sikkerhedsstandarder, inden systemet godkendes til brug. Når et system er registreret, bliver en systemejer udpeget. Det er systemejerens opgave at sikre, at systemet anvendes i henhold til Atea´s databeskyttelsesregler, navnlig med fokus på administration af adgangsrettigheder.

Dataklassificering
For at sikre at oplysninger, der opbevares uden for et godkendt it-system administreres på det fornødne sikkerhedsniveau, skal Atea´s medarbejdere sørge for at mærke filer, dokumenter eller e-mails, der indeholder oplysninger i forhold til, hvor følsomme oplysningerne er, således at det er nemt for alle modtagere at se. Mærkningen skal følge Atea´s regler for klassificering af data.

Alle rutiner for behandling af personoplysninger skal desuden dokumenteres og gennemgås af it-sikkerhedschefen. Hver af Atea´s ledere er tilknyttet en Databeskyttelsesadministrator, som er ansvarlig for en specifik funktion i den pågældendes land (eller serviceenhed). Det er databeskyttelsesadministratorens opgave at påse, at alle forretningsprocesser inden for vedkommendes funktion overholder Atea´s databeskyttelsesregler, i henhold til databeskyttelsesforordningen.

Administration af personoplysninger
Når vi indsamler personoplysninger, skal vi underrette den enkelte person eller indhente samtykke til, at vedkommendes personoplysninger indsamles og bruges, i henhold til databeskyttelsesforordningen. Der er mange oplysningskrav i databeskyttelsesforordningen vedrørende indholdet af meddelelsen (se brødtekst). Konsulter altid Atea landets DPO før opgaven påbegyndes; nogle virksomheder eller personer kan opgive fejlagtige informationer og/eller fortolke GDPR juridisk forkert.

Brud på datasikkerheden er et brud på informationssikkerheden, der medfører, at uautoriserede personer får adgang til data, eller resulterer i ulovlige eller utilsigtede tab af data. Atea har særlige forpligtelser i henhold til databeskyttelsesforordningen i tilfælde af brud på datasikkerheden i forbindelse med personoplysninger.

I tilfælde af mistanke om brud på datasikkerheden skal Atea´s medarbejdere straks underrette it-sikkerhedschefen for deres land eller serviceenhed. Der kan også sendes en e-mail til infosec@atea.com, som bliver videresendt til Atea-koncernens øverste it-sikkerhedsansvarlige.

Atea skal i henhold til databeskyttelsesforordningen have indgået en databehandlingsaftale med sine kunder, når kundens datainfrastruktur og applikationer administreres. Atea skal også have indgået en databehandlingsaftale med sine underleverandører eller leverandører, der behandler data på vegne af Atea. Der er mange oplysningskrav i databeskyttelsesforordningen vedrørende indholdet af databehandlingsaftalen (se brødtekst).

4. BESKYTTELSE AF IT-INFRASTRUKTUR – OBLIGATORISK PRAKSIS FOR ALLE MEDARBEJDERE

Atea´s it-infrastruktur består af al hardware, software og netværkskomponenter, der understøtter leveringen af forretningssystemer og it-relaterede processer til brugerne. Databeskyttelse hos Atea er afhængig af, at alle medarbejdere anvender Atea´s it-infrastrukturer på en ansvarlig måde.

Følgende regler gælder for alle medarbejdere hos Atea, som er brugere af Atea´s it-infrastruktur, og omfatter enhedssikkerhed, systemadgang, fillagring, netværkssikkerhed, kommunikation og fysisk sikkerhed. Derudover skal medarbejdere med ansvar for administration af Atea´s it-drift tage særskilte og mere omfattende træningskurser i it-sikkerhed svarende til deres funktion.

Device sikkerhed:
Atea´s medarbejdere skal træffe sikkerhedsforanstaltninger i forhold til sine IT-arbejdsenheder, som f.eks. pc'er, tablets og smartphones. Disse enheder er særligt udsat for tyveri, malware og uautoriseret brug. Atea´s pc'er, tablets og smartphones skal altid holdes under opsyn eller opbevares på et sikkert sted. Når enhederne ikke er i brug, skal de være låst med PIN-/adgangskode eller slukket.

Alle Atea´s pc'er, tablets og smartphones skal have krypteringsløsninger installeret for at forhindre uautoriseret adgang til harddisken. Atea´s Windows pc'er aktiveres ved hjælp af Bitlocker-kryptering. På Apple Mac-modeller er der en indbygget funktion til at kryptere harddisken, som skal aktiveres ved brug. Alle iPhone- og iPad-enheder har fra fabrikken kryptering installeret. Kryptering skal aktiveres manuelt på Android-mobiler og tablets. Kryptering skal også aktiveres på flytbare hukommelseskort og USB-drev, der nemt kan gå tabt. Medarbejdere, der har brug for hjælp til kryptering af deres arbejdsenheder, kan kontakte Atea Servicedesk.

Atea´s medarbejdere må ikke downloade software på deres pc'er, der ikke er købt hos Atea´s it-afdeling. Atea´s it-afdeling tilbyder en række softwareprogrammer via deres ServiceMarket (Accelerator) portal. Disse programmer opdateres regelmæssigt for at opretholde det korrekte sikkerhedsniveau. Hvis Atea´s medarbejdere skal hente ekstern software til sin pc, som ikke er fra ServiceMarket (Accelerator) portalen, skal de først have godkendelse fra deres chef og fra den lokale it-afdeling.

Atea´s pc'er har antimalware (virus) beskyttelse og firewall-programmer installeret. Hvis du er i tvivl om din antimalware-beskyttelse, kan du kontakte Atea Servicedesk. Hvis du modtager en antimalware-advarsel, eller hvis din computer ikke fungerer optimalt, kan det være tegn på, at din computer er blevet kompromitteret. Tegn på malware på en pc kan f.eks. være, at pc'en ofte fryser eller er utrolig langsom, eller at aktiviteter sker af sig selv, herunder popups eller andre ændringer på skærmen.

Hvis du har mistanke om, at din pc er blevet kompromitteret, skal du først indstille alt arbejde på computeren og frakoble nettet. Kontakt derefter Atea Servicedesk, og oplys, hvilke symptomer der ligger til grund for mistanken om, at pc'en har været udsat for malwareangreb, og hvad der kan have ført til, at pc'en er blevet kompromitteret.

Alle arbejdsenheder, der tages ud af brug, skal renses for data, før de sendes til service, genindvinding eller genanvendelse fra Atea. Dette skal ske i overensstemmelse med de it-procedurer, der er iværksat i hvert land.

Systemadgang:
Atea´s medarbejdere bør kun gives adgang til systemer, når det er nødvendigt i deres arbejde. Adgangsrettigheder til systemer skal hele tiden screenes for at sikre, at denne regel bliver overholdt, og at adgangen ophører, så snart den ikke længere er nødvendig. Hvis Atea´s medarbejdere har adgang til systemer, som de ikke længere har brug for, skal de straks kontakte systemejeren for at annullere/disable deres adgangsrettigheder.

Når en af Atea´s medarbejdere gives ret til adgang, skal brugernavn og midlertidig adgangskode udleveres separat – to forskellige kanaler. Den midlertidige adgangskode skal ændres umiddelbart efter første login og bør ikke skrives ned

eller deles med andre. Medarbejderne må ikke overdrage adgangsrettigheder til andre brugere.

Fillagring:
Alle Atea´s medarbejdere skal sikre, at deres arbejdsfiler (f.eks. MS Word/Excel/Powerpoint filer) håndteres sikkert. Alle typer filer skal gemmes på Atea´s fælles filservere, OneDrive eller i Sharepoint. Der må ikke anvendes andre eksterne lagringsløsninger, herunder Dropbox eller Google Drev, til at opbevare Atea´s filer uden udtrykkelig tilladelse fra det pågældende lands it-afdeling, idet Atea ikke kan garantere sikkerheden for disse lagringsløsninger. Atea´s medarbejdere må ikke gemme virksomhedsoplysninger på sine lokale enheders harddiskdrev, da disse oplysninger ikke sikkerhedskopieres automatisk og derfor er i fare for datatab.

Filerne skal være mærket i overensstemmelse med Atea´s dataklassificeringsregler (De 5 niveauer). Filer, der er mærket som strengt fortrolige, skal opbevares krypteret. Filer, der indeholder personoplysninger, skal også mærkes og opbevares i henhold til databeskyttelsesforordningen.

Atea´s medarbejdere skal være meget forsigtige, når de gemmer personoplysninger som følge af de strenge krav til databeskyttelse i databeskyttelsesforordningen. Medarbejderne må ikke bruge personoplysninger i filer til andet end det oprindelige formål, som er defineret og kommunikeret til personen, hvis oplysninger er indsamlet. Medarbejderne skal begrænse deling af filer indeholdende personoplysninger for at undgå misligholdelse eller misbrug af disse oplysninger og skal slette personoplysningerne, så snart de ikke længere er nødvendige. Dette gælder for alle filer, som Atea´s medarbejdere opretter - herunder MS Word/Excel/Powerpoint filer.

Netværkssikkerhed:
Kun Atea´s (PC) klienter (computere konfigureret iht. Atea Standard) må oprette forbindelse til Atea´s domæne. Atea´s mobile enheder skal kun oprette forbindelse til Atea´s WiFi-netværk for mobile enheder. Andre computere eller mobile enheder henvises til Atea´s WiFi-netværk for gæster.

Atea tilbyder medarbejdere uden for kontoret mulighed for tilslutning til det interne netværk via Cisco VPN eller Citrix. Dette giver adgang til vores fælles filsystem samt vores almindelige virksomhedssystemer. For at tilslutte til Cisco VPN skal computeren tilhøre Atea, være medlem af Atea´s domæne (ONE) og have antimalware software installeret.

Atea´s medarbejdere må aldrig tilslutte til en kundes netværk uden forudgående tilladelse fra kunden, medmindre andet fremgår af kundeaftalen. Kunden skal kontaktes hver gang, en af Atea´s medarbejdere tilslutter til deres netværk, og Atea´s medarbejder skal altid underrette kunden om, hvilke foranstaltninger vedkommende har truffet på kundernes netværk.

Atea´s medarbejdere skal være forsigtige, når de bruger et offentligt trådløst netværk. Datatrafik via offentlige netværk kan være overvåget. Før brug af et trådløst netværk skal Atea´s medarbejdere sikre sig, at netværket er sikret og kommer fra en pålidelig udbyder. Hvis der er nogen som helst grund til at betvivle sikkerheden på et offentligt trådløst netværk, skal Atea´s medarbejdere i stedet bruge det mobile netværk. Atea Servicedesk yder support til tilslutning af pc til det mobile netværk.

Det forventes, at Atea´s medarbejdere skal bruge internettet i deres daglige arbejde. Privat brug af internet er tilladt, men bør begrænses til sider med indhold, som er relevant for arbejdspladsen. Onlinespil eller pengespil er ikke tilladt, og fildeling eller mediestreaming via internettet skal begrænses til arbejdsrelateret indhold. Alle medarbejdere skal være opmærksomme på, at Atea analyserer trafikken på internettet for at registrere eventuelle angreb mod Atea, hvilket også vil afsløre utilbørlig brug af internettet.

Når du besøger hjemmesider på internettet, skal du være varsom med, at hjemmesiden er korrekt - især hvis du omdirigeres fra en anden side. Klik aldrig på link eller popups på internetsider, hvis de ser mistænkelige ud, da de kan indeholde malware, som kan indlæses på din enhed.

Kommunikation (e-mail/sociale medier):
E-mail er et vigtigt digitalt kommunikationsværktøj for Atea´s medarbejdere. Det er også en

væsentlig kilde til sårbarhed i forhold til informationssikkerhed, da det giver svindlere mulighed for at rette angreb mod Atea med malware, svindel og andre trusler, til en billig penge og med minimal risiko for at blive retsforfulgt.

En hyppig form for identitetssvindel ("phishing") mod Atea er, når en af Atea´s medarbejdere får tilsendt en e-mail direkte fra svindleren. E-mailen kommer tilsyneladende fra en pålidelig kilde, ofte ved hjælp af en falsk identitet som f.eks. en anden Atea-medarbejder, en forretningsforbindelse eller en leverandør, som f.eks. en teknologivirksomhed eller en bank. E-mailen forsøger at narre Atea-medarbejderen til at svare, f.eks. i form af at foretage pengeoverførsler, indtaste login/adgangskode eller andre følsomme oplysninger, eller til at klikke på et link eller en vedhæftet fil, der downloader ondsindede programmer (også kaldet "malware") på brugerens pc eller mobil.

Mailen, den vedhæftede fil eller linket ser ud til at være helt uskyldigt - udgiver sig f.eks. for at være en mail fra en kollega, et tilbud/faktura fra en leverandør eller en meddelelse fra en Cloud-konto såsom OneDrive. Derfor skal Atea´s medarbejdere være meget på vagt overfor risikoen for svindel i e-mails eller anden kommunikation, selvom det tilsyneladende kommer fra en pålidelig kilde.

Atea´s medarbejdere bør aldrig åbne vedhæftede filer eller link fra deres enheder, hvis der er tvivl om en mails eller meddelelses pålidelighed. Hvis en medarbejder er i tvivl om en e-mails pålidelighed, eller hvis vedkommende ved et uheld har reageret på et potentielt forsøg på svindel ved at åbne et mistænkeligt link eller en vedhæftet fil, skal Atea Servicedesk straks kontaktes og forholdet anmeldes.

Medarbejderes mailkonti bliver ofte angrebet af svindlere, som forsøger at få adgang til medarbejdernes virksomhedsfølsomme filer. Derfor må e-mail ikke benyttes til lagring af vigtige virksomhedsoplysninger. Virksomhedens oplysninger skal opbevares eller videregives via sikrede systemer eller fildelingsløsninger fremfor e-mail.

Privat brug af e-mail er tilladt, forudsat det ikke er i strid med Atea´s forretningsinteresser eller griber forstyrrende ind i arbejdstiden. Privat mailkorrespondance bør altid være relevant for arbejdspladsen og skal være mærket "privat". Desuden må brug af virksomhedens e-mailkonto til personlig korrespondance ikke efterlade det indtryk, at korrespondancen kommer fra eller er godkendt af Atea.

Sociale medier er også et hyppigt anvendt kommunikationsværktøj for Atea´s medarbejdere. Når de sociale medier anvendes korrekt, giver de Atea´s medarbejdere mulighed for at tilegne sig og formidle viden til opbygning af forretningsforbindelser og styrkelse af Atea´s brand. På den anden side kan de sociale medier være meget ødelæggende for Atea og deres medarbejdere, hvis de anvendes uhensigtsmæssigt, eller hvis følsomme oplysninger deles.

Atea´s medarbejdere bør derfor være meget forsigtige med, hvilke oplysninger de deler på de sociale medier. Alle personlige oplysninger (herunder navn, fotos m.v.) må kun deles via opslag på de sociale medier med tilknytning til Atea´s forretning, hvis personen, hvis oplysninger bliver delt, giver tilladelse til brug af oplysningerne.

Det er ikke tilladt at tage et billed af sit fysiske adgangskort til Atea´s bygninger og uploade det på de sociale medier; adgangskortet kan derved nemt kopieres.

Sikkerhed på kontoret:
Atea´s medarbejdere bør bære synligt adgangs/personalekort for identifikation. Alle besøgende hos Atea skal registreres i receptionen og udstyres med et gæstekort, der skal bæres synligt eller den besøgende skal følges af en Atea ansat. Besøgende bliver afhentet i receptionen, når besøget starter, og fulgt tilbage til receptionen for at aflevere deres gæstekort (hvis udleveret), når besøget er slut. Besøgende må ikke efterlades alene i Atea´s bygninger.

Alle følsomme oplysninger bør fjernes fra skriveborde og opbevares forsvarligt, når de ikke er i brug. Alle tavler skal viskes rene for oplysninger, når møder er afholdt. Fortrolige dokumenter skal altid destrueres i makulator eller smides i særlige skraldespande, hvis de ikke længere skal bruges.

Sammenfatning
- Beskyttelse af it-infrastruktur:

Enhedssikkerhed:
Alle Atea´s pc'er, tablets og smartphones skal have krypteringsløsninger installeret for at forhindre uautoriseret adgang til harddisken. Atea´s pc'er, tablets og smartphones skal altid holdes under opsyn eller opbevares på et sikkert sted. Når enhederne ikke er i brug, skal de være låst med PIN-/adgangskode eller slukket.

Atea´s medarbejdere må ikke downloade software på deres pc'er, der ikke er købt hos Atea's it-afdeling. Hvis Atea´s medarbejdere skal hente ekstern software på deres pc, som ikke er fra Atea, skal de først have godkendelse fra deres chef og fra den lokale it-afdeling.

Atea´s pc'er har antimalware og firewall-programmer installeret. Hvis du er i tvivl om din antimalware-beskyttelse, kan du kontakte Atea Servicedesk.

Hvis du har mistanke om, at din pc er blevet inficeret med malware eller er blevet kompromitteret, skal du først indstille alt arbejde på computeren og frakoble nettet. Kontakt derefter Atea Servicedesk.

Systemadgang:
Atea´s medarbejdere bør kun gives adgang til systemer, når det er nødvendigt i deres arbejde. Adgangsrettigheder til systemer skal hele tiden screenes for at sikre, at denne regel bliver overholdt, og at adgangen ophører, så snart den ikke længere er nødvendig.

Fillagring:
Alle Atea´s medarbejdere skal sikre, at deres arbejdsfiler (f.eks. MS Word/Excel/Powerpoint filer) håndteres sikkert. Filerne skal være mærket i overensstemmelse med Atea´s dataklassificeringsstandarder (5 niveauer), med særskilt mærkning af filer indeholdende personoplysninger. Filer, der er mærket som fortrolige, skal opbevares krypteret.

Alle typer filer skal gemmes på Atea´s fælles filservere, OneDrive eller i Sharepoint. Der må ikke anvendes andre eksterne lagringsløsninger, herunder Dropbox eller Google Drev, til at opbevare Atea´s filer uden udtrykkelig tilladelse fra det pågældende lands it-afdeling. Atea´s medarbejdere må ikke opbevare virksomhedsoplysninger på deres lokale enheders harddiskdrev.

Netværkssikkerhed:
Kun Atea´s klienter (computere konfigureret iht. Atea Standard) må oprette forbindelse til Atea´s domæne. Atea´s mobile enheder skal kun oprette forbindelse til Atea´s WiFi-netværk for mobile enheder. Andre computere eller mobile enheder henvises til Atea´s WiFi-netværk for gæster.

Atea´s medarbejdere skal være forsigtige, når de bruger et offentligt trådløst netværk. Før brug af et trådløst netværk skal Atea´s medarbejdere sikre sig, at netværket er sikret og kommer fra en pålidelig udbyder.

Adgang til internettet fra en arbejdsenhed bør begrænses til sider med indhold, som er relevant for arbejdspladsen. Alle medarbejdere skal være opmærksomme på, at Atea analyserer trafikken på internettet for at registrere eventuelle angreb mod Atea, hvilket også vil afsløre utilbørlig brug af internettet.

Når du besøger hjemmesider, skal du være varsom med, at hjemmesiden er korrekt - især hvis du omdirigeres fra en anden side. Klik aldrig på link eller popups på internetsider, hvis de ser mistænkelige ud, da de kan indeholde malware, som kan indlæses på din enhed.

Kommunikation (e-mail/sociale medier):
E-mail er også en væsentlig kilde til sårbarhed i forhold til informationssikkerhed, da det giver svindlere mulighed for at rette angreb mod Atea med malware, svindel og andre trusler, til en billig penge og med minimal risiko for at blive retsforfulgt.

En hyppig form for identitetssvindel ("phishing") mod Atea er, når en af Atea´s medarbejdere får tilsendt en e-mail direkte fra svindleren. E-mailen kommer tilsyneladende fra en pålidelig kilde, ofte ved hjælp af en falsk identitet som f.eks. en anden Atea-medarbejder, en forretningsforbindelse eller en leverandør, som f.eks. en teknologivirksomhed eller en bank. E-mailen forsøger at narre Atea-medarbejderen til at svare, f.eks. i form af at foretage pengeoverførsler, indtaste login/adgangskode eller andre følsomme oplysninger, eller til at klikke på et link eller en vedhæftet fil, der downloader ondsindede programmer (også kaldet "malware") på brugerens pc eller mobil.

Atea´s medarbejdere bør aldrig åbne vedhæftede filer eller link fra deres enheder, hvis der er tvivl om en mails eller meddelelses pålidelighed. Hvis en medarbejder er i tvivl om en e-mails pålidelighed, eller hvis vedkommende ved et uheld har reageret på et potentielt forsøg på svindel ved at åbne et mistænkeligt link eller en vedhæftet fil, skal Atea Servicedesk straks kontaktes og forholdet anmeldes.

Privat brug af e-mail er tilladt, forudsat det ikke er i strid med Atea´s forretningsinteresser eller griber forstyrrende ind i arbejdstiden. Privat mailkorrespondance bør altid være relevant for arbejdspladsen og skal være mærket "privat".

Atea´s medarbejdere bør være meget forsigtige med, hvilke oplysninger om Atea de deler på de sociale medier. Alle personlige oplysninger (herunder navn, fotos m.v.) må kun deles via opslag på de sociale medier med tilknytning til Atea, hvis personen, hvis oplysninger bliver delt, giver tilladelse til brug af oplysningerne.

Sikkerhed på kontoret:
Atea´s medarbejdere bør bære synligt personalekort for identifikation. Alle besøgende hos Atea skal registreres i receptionen og udstyres med et gæstekort, der skal bæres synligt. Alle følsomme oplysninger bør fjernes fra skriveborde og opbevares forsvarligt, når de ikke er i brug.

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

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

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

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

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

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

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

Group Shared Services
Atea Global Services SIA
Mukusalas Street 15
LV-1004 Riga
+371 67359600
Virk.nr. 50203101431
rigainfo@atea.com
ateaglobal.com

ATEA