PlanAHead A/S og Databeskyttelsesloven

Version GDPR 19.11.20

Indledning

PlanAHead A/S leverer vagtplanlægningsløsninger til kunder med intern IT og leverer drift af SQL server databaser samt Aplanner for Web for kunder. Vi har som virksomhed forberedt os på at opfylde kravene i Databeskyttelsesloven og at hjælpe vore kunder med at opfylde kravene. Dette dokument giver et overblik over de tiltag, vi har foretaget så dokumentet kan danne basis for databehandleraftaler med vore kunder.

Ledelsessystem og sikkerhed hos PlanAHead A/S

PlanAHead A/S har en beskrevet proces for behandling kundeoplysninger og det IT-udstyr, vi anvender. De vigtigste elementer er:

- Vore kundedatabaser er placeret på Microsoft Windows Azure virtuelle servere lokaliseret i Nordeuropa. Driften af disse servere inkluderer løbende opgradering til nyeste software, skift af adgangskoder med løbende mellemrum, samt regler om anvendelse af firewalls og virus beskyttelse.
- Backup af vores kunde databaser gemmes på et Microsoft Windows Azure lager. Driften af dette lager inkluderer kryptering af dataforbindelse og data samt skift af adgangskode med løbende mellemrum. Backups gemmes i max 180 dage.
- Der gemmes kundedata drevet af kundebehov for support på vores udviklingsmaskine, som er en bærbar PC. Der er kun adgang til udviklingsmaskinen fra en enkelt Microsoft netværkskonto. Lageret på den bærbare PC er krypteret med Bitlocker. Adgangskoden netværkskontoen skiftes med løbende mellemrum. Kundedata til brug for support slettes efter brug.

Hjælp til vore kunder i Aplanner for Windows

Der findes en række værktøjer i Aplanner for Windows som administrator hos vore kunder kan benytte sig af for at leve op til databeskyttelsesloven:

- Der findes et adgangssikkerhedssystem som kan tildele rettigheder til den enkelte bruger efter behov. Brugerne kan selv skifte adgangskode.
- Alle database oplysninger, der vedrører en medarbejder kan dokumenteres ved anvendelse af de to rapporter Timetabel og Udskrift af stamdata samt billedet Redigering af Synkroniseringsdata. Begge rapporter dannes som HTML sider. Synkroniseringsoplysningerne kan filtreres og kopieres.
- Fjernelse af alle data vedrørende en medarbejder kan udføres i to trin, først slettes medarbejderen fra stamdata kataloget. Herefter udføres databasefunktionen fjern slettede objekter. Hvis databasen er placeret hos PlanAHead A/S vil backup data af medarbejderens oplysninger forsvinde efter max 180 dage.
- Vagtplanlægningsløsningen har kun et enkelt interface til andre systemer, nemlig synkronisering af vagter via Outlook. Der gemmes kopi af udsendte kalenderposter i databasen.

Hjælp til vore kunder, der har placeret databasen hos PlanAHead A/S

Vi tilbyder følgende, som kan hjælpe med opfyldelse af databeskyttelseslovens krav:

- Datatrafikken mellem Aplanner for Windows og databasen krypteres.
- Adgangskoder krypteres inden forsendelse.
- Efter anmodning kan PlanAHead A/S slette eller tilbagelevere kundedatabaser
- Adgang til Aplanner for Web er krypteret og serveren har et SSL-certifikat.
- Al programkode fra PlanAHead A/S er certificeret med et Code Sign certifikat.
- Den sikkerhedsansvarlige hos PlanAHead A/S kan logge sig på en kundedatabase, hvis der opstår et supportbehov.

Begrænsninger

- PlanAHead A/S har ikke mulighed for at hjælpe med kontrol af oplysninger, som er sendt via synkroniseringen. Her henvises til kundes mail og kalendersystem.
- Aktive databaser placeret på virtuelle servere er ikke krypteret. Det betyder i praksis, at PlanAHead's database administrator kan se kundedata, bortset fra adgangskoder, som er krypteret.
- PlanAHead A/S har valgt Microsoft Windows Azure som leverandør af virtuelle servere på standard betingelser (Pay-As-You-Go). Dette valg er ufravigeligt.
- PlanAHead A/S anvender Microsoft Windows Azure backup system. Hvis kunden ønsker det kan PlanAHead A/S lukke for backup og muliggøre, at kunden selv laver en backup fra Aplanner for Windows (Gem som XML-fil).
- Der findes ikke felter i databasen til lagring af CPR-oplysninger eller lignende følsomme personoplysninger. Hvis kunden ønsker at lagre personfølsomme oplysninger i vagtplanlægningsløsningen, tilråder vi at kunden bestiller en opgradering af databasesikkerheden, f.eks. til fuld kryptering af databasen.