IT-SIKKERHED HOS MOBILIZE ME APS

En gennemgang til kommuner

Mobilize Me ApS, Åbogade 15, 8200 Aarhus N

Indholdsfortegnelse

INDLEDNING

I dette dokument tager vi jer igennem en række sikkerhedsmæssige overvejelser, som er forbundet med at implementere Mobilize Me ApS' værktøjer i en kommune.
Vejledningen er bygget således op, at vi indleder med at besvare de spørgsmål, som vi oftest bliver mødt af hos kommunerne. Spørgsmålene er overvejende af teknisk art og vedrører selve systemets opbygning.
Herefter beskriver vi, hvilke ansvarsområder, der bør uddelegeres, inden værktøjet tages i anvendelse. Dette handler primært om, at I som kommunen bør sikre jer, at nogen tager ansvar for den daglige håndtering af administrationsopgaver, som er forbundet med værktøjet.
Til sidst beskriver vi en række procedurer, som skal hjælpe jeres personale med at håndtere værktøjet i dagligdagen på den bedste – og sikreste måde. Heri indgår bl.a. også retningslinjer for daglig brug af værktøjet ift. personfølsomme oplysninger og personhenførbart data.
Skulle I have yderligere spørgsmål, så kontakt os gerne på: kontakt@mobilize-me.com

---

IT-SIKKERHED HOS MOBILIZE ME APS - FAQ

1. Ligger det borgerrelaterede indhold lokalt på iPad /smartphone?
Ja, der ligger lokalt indhold på borgernes device, fordi det har vist sig som et konkret behov, at borgerne kan tilgå deres data i offline tilstand. De oplysninger, som ligger cached, er dog ikke nødvendigvis personhenførbare data, og de bliver udelukkende lagt ind af borgernes relaterede ressourcepersoner og fagpersonale. Oplysningerne kan f.eks. være "Indkøb i brugsen" eller "Legeaftale med Mikkel", med understøttende billeder heraf. Når borgerne logger sig ud af værktøjet, bliver alle cachede oplysninger slettet.

2. Eller er indholdet udelukkende lagret centralt på en server / cloudløsning?
Mobilize Me ApS lagrer oplysningerne centralt i en cloudløsning i Danmark på nationale servere. Dermed bliver relevante data synkroniseret med borgerens device, når borgeren har brug for dem.

3. Vil registrerede personoplysninger være beskyttede i Mobilize Me ApS' sikkerhedsforanstaltninger, i henhold til Persondataloven og Sikkerhedsbekendtgørelsen og dennes vejledning?
Ja, vores centrale leverandør er underlagt revision af ISO27000 og fællesstatslige standard for informationssikkerhed (DS484)

4. Hvordan er de supplerende tekniske sikkerhedsforanstaltninger for personfølsomme oplysninger?
Vi logger alle aktiviteter på vores system - fx transaktionslogning og logning af afviste adgangsforsøg. Derudover er der mulighed for differentiering på roller og rettigheder, hvis der er et fagligt behov for det.

5. Anvendes der stærk kryptering over åbne netværk?
Ja, der er SSL-kryptering af al trafik.

6. Hvor høj kryptering bruger I?
Vi bruger en 2048 bit krypteringsnøgle.

7. Hvem hoster de data, der benyttes af Mobilize Me ApS?
Vores leverandør er Cloud.dk - deres sikkerhed bliver beskrevet på følgende side:
http://www.cloud.dk/da/teknik/sikkerhed

8. Hvis dataanmeldelse er et krav fra vores kommune, er det så noget I gør?
Ja, vi udarbejder gerne en dataanmeldelse med den pågældende kommune

9. De oplysninger, der registreres ifm. den enkelte persons licens, er de beskyttet af anerkendte sikkerhedsforanstaltninger?
Ja, Mobilize Me ApS benytter sig af e-conomic, som er et anerkendt regnskabsprogram, der også vægter datasikkerhed højt og som årligt overholder revisionsstandarden RS 3000.
Deres sikkerhed bliver beskrevet på følgende side:
http://www.e-conomic.dk/regnskabsprogram/sikkerhedteknik/sikkerhed

BRUGERSTYRING

Lokal administrator: Vi anbefaler, at man udvælger en eller flere lokale administratorer, som har adgang til at oprette, nedlægge og redigere i brugernes profiler. Ved at have lokale administratorer sikrer I jer, at der kan foretages en hurtig og effektiv reaktion, hvis der sker noget uventet, som fx tab af udstyr.
Central brugerstyring: Hvis kommunen i forvejen anvender et centralt styresystem, kan man selvfølgelig også lægge administratorrettighederne der. Det er dog vigtigt, at tage stilling til, hvem der står for administrationen, så det er tydeligt for personalet, hvem de skal henvende sig til, når de har brug for ændringer.
Hvis I skulle have brug for et tilbud på integrering af værktøjer fra Mobilize Me ApS til jeres eksisterende systemer, så kontakt os gerne.

SYSTEMEJER

Det er vigtigt at udpege en systemejer, som er ansvarlig for it-sikkerhed, drift, vedligeholdelse og kontraktlige forhold ift. Mobilize Me ApS. Systemejeren tager ansvar for at holde sig opdateret ift. retningslinjer for brug af værktøjet og holde personalet ajour med opdateringer, ændringer mm.
Se mere herom på digitaliseringsstyrelsens hjemmeside.

DATABEHANDLERAFTALE

Det er Mobilize Me ApS' klare anbefaling, at vi indgår en databehandleraftale ifm. samarbejdet. I en databehandleraftale overtager vi ansvaret for den data, som opbevares på vores servere, og I undgår dermed ansvaret for noget, I ikke har kontrol over. Det synes vi, giver bedst mening for alle.

BRUGEN AF PASSWORD

Som i alle andre systemer, er det selvfølgelig vigtigt, at brugerne ændrer passwordet, så det bliver personligt. Det kan man gøre inde i app'en.
Et stærkt password indeholder disse elementer:

- Er minimum 8 tegn langt
- Indeholder både små og store bogstaver
- Indeholder tal
- Indeholder specialtegn (&%#)

PINKODEBESKYTTELSE AF DEVICES

Vi opfordrer derudover kraftigt til, at brugeren benytter sig af pinkode eller touch ID på sin device. Skulle det ske, at brugeren mister sin device, imens vedkommende er logget ind, vil en tredjepart kunne åbne app'en og få adgang til brugerens data - indtil brugerkontoen er lukket.

PERSONFØLSOMME OPLYSNINGER

Mobilize Me ApS' værktøjer er lavet til at kunne håndtere personfølsomme oplysninger, men det er ikke formålet med dem. Vi anbefaler derfor, at man ikke bevidst lægger oplysninger ind i værktøjet, som vedrører borgerens personfølsomme oplysninger såsom:

- Oplysninger om helbredsforhold
- Straffeattest og andre tilsvarende rent private forhold
- Personlighedstest m.v.
- Racemæssig eller etnisk baggrund
- Politisk, religiøs eller filosofisk overbevisning
- Seksuelle forhold
- Væsentlige sociale problemer

PERSONHENFØRBARE DATA

I sin korte form, dækker personhenførbare data over informationer, som med rimelighed kan forventes at føre tilbage til en fysisk person. Det kan fx være identifikationsoplysninger (navn, adresse osv.) eller familieforhold. Disse oplysninger er ikke følsomme, men de skal alligevel behandles med omhu. Vi anbefaler, at man for så vidt muligt undgår at lægge personhenførbare data ind i værktøjet, men nøjes med oplysninger som relaterer sig til borgerens brug af værktøjet.

BRUG AF BILLEDER

Billeder er en stor del af Mobilize Me ApS' værktøjer og et særdeles effektivt virkemiddel ift. vores brugere. Det er dog vigtigt, at personalet har for øje, at der ikke må indgå personfølsomme oplysninger, når der tages billeder.

Personalet må fx ikke tage billeder af:
- Et pilleglas, hvor der er påtrykt et CPR-nummer
- Et religiøst tidsskrift
- En kuvert/et dokument med navn og adresse

SAMTYKKEERKLÆRINGER

Hvis der er brug for at tage et billede af en anden person, er det vigtigt at man har et samtykke fra ham/hende. Personen skal være bevidst om, at han/hun bliver fotograferet, og man kan med fordel indhente en samtykkeerklæring.

Man må gerne tage et billede af en forsamling (til en fest, et kursus eller lignende), uden at indhente samtykke, så længe der ikke er enkelte personer i fokus.

TEKSTBESKEDER

Generelt gælder der de samme retningslinjer for tekstbeskeder, som for brug af billeder: Skriv ikke om personfølsomme oplysninger og undgå for så vidt muligt personhenførbar data.

PROCES FOR AKTINDSIGT

Hvis en borger beder om aktindsigt hos sin støtteperson, henvender denne sig til den lokale administrator. Han eller hun tager skriftlig kontakt til Mobilize Me ApS og beder om de relevante data. Vi leverer data tilbage, som sendes i en sikker mail direkte til borgeren.

PROCES FOR BORTKOMMET UDSTYR

Skulle det ske, at en bruger mister sin device, skal der tages kontakt til den lokale administrator, som sørger for at deaktivere brugeren profil. Alle brugerens data forbliver gemte på vores server, men man vil ikke kunne logge ind på brugerens profil, før den aktiveres igen.

Skulle det ske, at devicen er offline, kan vi ikke nå den, og man vil derfor kunne tilgå kontoens dagsstruktur, indtil der igen er netforbindelse.