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 kommune 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 værktøjerne ift. følsomme personoplysninger og personhenførbare 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?
Der kan i enkelte tilfælde ved brug af Mobilize Me ligge indhold lokalt på borgerens device. Dette skyldes, at der for lige præcist borgere, der bruger Mobilize Me, 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. Hvordan er de supplerende tekniske sikkerhedsforanstaltninger for følsomme personoplysninger?
Vi logger alle aktiviteter på vores system - fx transaktionslogning og logning af afviste adgangsforsøg.

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

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

6. Hvem hoster de data, der benyttes af Mobilize Me ApS?
Vores leverandør er Curanet.dk - deres sikkerhed bliver beskrevet på følgende side: https://curanet.dk/om-os/compliance. Ved henvendelse kan I få tilsendt en ISAE3402 erklæring fra Curanet.

7. Hvis en databehandleraftale er et krav fra vores kommune, er det så noget I gør?
Mobilize Me Aps. udarbejder gerne en databehandleraftale med alle kommuner der ønsker en sådan.

8. De oplysninger, der registreres ifm. køb af licens, er de beskyttet af anerkendte sikkerhedsforanstaltninger?
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

Brug af Mobilize Me's værktøjer kræver, at man som institution, skole eller kommune udvælger en eller flere lokale administratorer, som uddannes til superbrugere og får adgang til at oprette, nedlægge og redigere i brugernes profiler.

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.
Systemejeren bliver indskrevet i Databehandleraftalen.

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.

FØLSOMME PERSONOPLYSNINGER

Mobilize Me ApS's værktøjer har til formål at hjælpe borgere med udfordringer med at lægge struktur. Brugen af Mobilize Me's værktøjer er ikke betingede af, at der oplyses følsomme personoplysninger. Der er dog enkelte fritekstfelter, hvor der vil kunne lægges følsomme personoplysninger ind. Mobilize Me anbefaler, at man som udgangspunkt ikke lægger følsomme personoplysninger ind i værktøjet. Følsomme personoplysninger er defineret som:

- ☐ Race eller etnisk oprindelse.
- ☐ Politisk overbevisning.
- ☐ Religiøs overbevisning.
- ☐ Filosofisk overbevisning.
- ☐ Fagforeningsmæssigt tilhørsforhold.
- ☐ Genetiske data.
- ☐ Biometriske data.
- ☐ Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol m.v.

Hvis kommuner/institutioner, på trods af anbefalingerne fra Mobilize Me, ønsker at lægge følsomme personoplysninger ind i værktøjerne, anbefaler Mobilize Me, at kommunen/institutionen tager stilling til, hvordan kommunen alligevel kan opfylde betingelserne i databeskyttelsesforordningens artikel 9.

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 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 følsomme personoplysninger, 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 vedkommende. Personen skal være bevidst om, at vedkommende 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 følsomme personoplysninger og undgå personhenførbare data.

PROCES FOR AKTINDSIGT

Hvis en borger beder om aktindsigt hos sin støtteperson, henvender denne sig til den lokale administrator. Administratoren tager skriftlig kontakt til Mobilize Me ApS og beder om de relevante data. Mobilize Me sender de ønskede data i en sikker mail direkte til borgeren.

PROCES FOR BORTKOMMET UDSTYR

Mister en bruger sit device, skal der tages kontakt til den lokale administrator, som sørger for at deaktivere brugerens 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 devicet er offline, kan vi heller ikke komme i kontakt med det, og man vil derfor kunne tilgå kontoens dagsstruktur, indtil der igen er netforbindelse.